

Configuration Commands: a to f

- 24ghz-rf-policy default-dot11b-policy, on page 11
- 3gpp-info, on page 12
- aaa accounting identity, on page 13
- aaa accounting update periodic interval-in-minutes , on page 15
- aaa attribute list, on page 16
- aaa authentication dot1x, on page 17
- aaa authentication login, on page 18
- aaa authorization, on page 19
- aaa authorization credential download default, on page 23
- aaa authorization credential-download MY-METHOD-LIST group MY-SERVER-GROUP, on page 24
- aaa group server ldap, on page 25
- aaa group server radius, on page 26
- aaa local authentication default authorization, on page 27
- aaa new-model, on page 28
- aaa server radius dynamic-author, on page 30
- aaa session-id, on page 32
- access-session wireless cui-enable, on page 34
- aaa-override, on page 35
- aaa-override vlan fallback, on page 36
- aaa-policy , on page 37
- aaa-realm enable , on page 38
- absolute-timer, on page 39
- access-list, on page 40
- access-key (cloudwatch), on page 42
- access-list acl-ace-limit, on page 43
- accounting-list, on page 44
- acl-policy, on page 45
- active testing radio-selection always, on page 46
- action power-saving-mode power-profile, on page 47
- address, on page 48
- address, on page 50
- address-family ipv4, on page 51
- address prefix, on page 52

- advice-charge, on page 53
- advertise ap-name, on page 54
- airtime-fairness mode, on page 55
- allow at-least min-number at-most max-number, on page 56
- amsdu (mesh), on page 57
- anqp, on page 58
- anqp-domain-id, on page 59
- antenna beam-selection, on page 60
- antenna count, on page 61
- antenna monitoring, on page 62
- ap, on page 64
- ap audit-report, on page 65
- ap auth-list, on page 66
- ap auth-list ap-cert-policy allow-mic-ap , on page 67
- ap auth-list ap-cert-policy allow-mic-ap trustpoint, on page 68
- ap auth-list ap-cert-policy mac-address MAC-address | serial-number AP-serial-number policy-type mic, on page 69
- ap auth-list ap-policy, on page 70
- ap auth-list method-list MY-METHOD-LIST mac, on page 71
- ap capwap multicast, on page 72
- ap capwap retransmit, on page 73
- ap capwap timers, on page 74
- ap cisco-dna token, on page 76
- ap country, on page 77
- ap dot11 5ghz rrm channel unii3-low-power-channels, on page 78
- ap dot11 24ghz | 5ghz dot11ax spatial-reuse obss-pd , on page 79
- ap dot11 24ghz | 5ghz dot11ax spatial-reuse obss-pd non-srg-max , on page 80
- ap dot11 24ghz | 5ghz rrm ndp-mode, on page 81
- ap dot11 24ghz cleanair, on page 82
- default ap dot11 24ghz cleanair device, on page 83
- ap dot11 24ghz dot11g, on page 85
- ap dot11 24ghz rate, on page 86
- ap dot11 24ghz rf-profile default rf-profile, on page 88
- ap dot11 24ghz rrm channel cleanair-event, on page 89
- ap dot11 24ghz rrm channel device, on page 90
- ap dot11 24ghz rrm optimized-roam, on page 91
- ap dot11 24ghz rx-sop threshold, on page 92
- ap dot11 24ghz shutdown, on page 93
- ap dot11 5ghz channelswitch quiet, on page 94
- ap dot11 5ghz cleanair , on page 95
- default ap dot11 5ghz cleanair device, on page 96
- ap dot11 5ghz power-constraint, on page 97
- ap dot11 5ghz rate, on page 98
- ap dot11 5ghz rrm channel cleanair-event, on page 99
- ap dot11 5ghz rrm channel device, on page 100
- ap dot11 5ghz rrm channel zero-wait-dfs, on page 101

- ap dot11 5ghz rx-sop threshold, on page 102
- ap dot11 5ghz shutdown, on page 103
- ap dot11 5ghz smart-dfs, on page 104
- ap dot11 6ghz cleanair, on page 105
- ap dot11 6ghz rf-profile, on page 106
- ap dot11 , on page 107
- ap dot11 beaconperiod, on page 108
- ap dot11 cac media-stream, on page 109
- ap dot11 cac multimedia, on page 112
- ap dot11 cac voice, on page 113
- ap dot11 cleanair, on page 116
- ap dot11 cleanair alarm air-quality, on page 117
- ap dot11 cleanair alarm air-quality threshold, on page 118
- ap dot11 cleanair alarm device cont-tx, on page 119
- ap dot11 cleanair alarm unclassified, on page 120
- ap dot11 cleanair alarm unclassified threshold, on page 121
- ap dot11 cleanair device, on page 122
- ap dot11 dot11be, on page 124
- ap dot11 dot11n, on page 125
- ap dot11 dtpc, on page 128
- ap dot11 edca-parameters, on page 130
- ap dot11 load-balancing denial, on page 132
- ap dot11 load-balancing window, on page 133
- ap dot11 rf-profile, on page 134
- ap dot11 rrm, on page 135
- ap dot11 rrm channel, on page 138
- ap dot11 rrm channel cleanair-event, on page 139
- ap dot11 rrm channel dca, on page 140
- ap dot11 rrm channel-update mesh, on page 142
- ap dot11 rrm channel-update mesh bridge-group, on page 143
- ap dot11 rrm channel dca chan-width, on page 144
- ap dot11 rrm coverage, on page 145
- ap dot11 rrm group-member, on page 147
- ap dot11 rrm group-mode, on page 148
- ap dot11 rrm logging, on page 149
- ap dot11 rrm monitor, on page 151
- ap dot11 rrm ndp-type, on page 152
- ap dot11 rrm tpc-threshold, on page 153
- ap dot11 rrm txpower, on page 154
- ap dot11 rrm txpower, on page 155
- ap dot15 shutdown, on page 156
- ap file-transfer https port, on page 157
- ap filter , on page 158
- ap fra, on page 159
- ap fra 5-6ghz, on page 160
- ap fra 5-6ghz freeze, on page 161

- ap fra 5-6ghz interval, on page 162
- ap geolocation derivation ranging, on page 163
- ap geolocation ranging all accurate, on page 164
- ap geolocation ranging site accurate, on page 165
- ap hyperlocation, on page 166
- ap image, on page 167
- ap image site-filter, on page 168
- ap image upgrade, on page 169
- ap link-encryption, on page 170
- ap lsc-provision, on page 171
- ap lsc-provision renew due-time, on page 172
- ap lsc-provision renew one-shot, on page 173
- ap lsc-provision renew staggered, on page 174
- ap lsc-provision renew schedular, on page 175
- ap lsc renew due-time, on page 176
- ap name icap subscription ap rf spectrum, on page 177
- ap name antenna band mode, on page 178
- ap name ble, on page 179
- ap name clear-personal-ssid, on page 180
- ap name controller, on page 181
- ap name core-dump, on page 182
- ap name country, on page 183
- ap name crash-file, on page 184
- ap name dot11 24ghz | 5ghz | 6ghz rrm channel update mesh, on page 185
- ap name dot11 24ghz slot 0 SI, on page 186
- ap name dot11 24ghz slot antenna , on page 187
- ap name dot11 24ghz slot beamforming , on page 188
- ap name dot11 24ghz slot channel , on page 189
- ap name dot11 24ghz slot cleanair , on page 190
- ap name dot11 24ghz slot dot11n antenna, on page 191
- ap name dot11 24ghz slot dot11ax bss-color, on page 192
- ap name dot11 24ghz slot shutdown, on page 193
- ap name dot11 24ghz radio role manual sniffer channel, on page 194
- ap name dot11 5ghz radio role manual sniffer channel, on page 195
- ap name dot11 5ghz slot 1 dual-radio mode, on page 196
- ap name dot11 5ghz slot {1 | 2} urwb dfs , on page 197
- ap name dot11 5ghz slot {1 | 2} urwb ptmp base, on page 198
- ap name dot11 5ghz slot radio role, on page 199
- ap name dot11 channel width, on page 200
- ap name dot11 dual-band cleanair, on page 201
- ap name dot11 dual-band shutdown, on page 202
- ap name dot11 dual-band slot radio role manual client-serving, on page 203
- ap name dot11 dual-band slot shutdown, on page 204
- ap name dot11 dual-band slot band 6ghz, on page 205
- ap name dot11 rrm profile, on page 206
- ap name export support-bundle mode, on page 208

- ap name floor, on page 209
- ap name geolocation coordinate, on page 210
- ap name geolocation gnss antenna external cable-length, on page 211
- ap name geolocation height uncertainty, on page 212
- ap name hyperlocation, on page 213
- ap name image, on page 214
- ap name icap subscription client anomaly-detection report-individual enable aggregate, on page 215
- ap name icap subscription client anomaly-detection report-individual per-client throttle, on page 216
- ap name icap subscription client anomaly-detection report-individual per-type throttle, on page 217
- ap name indoor, on page 218
- ap name iot-radio firmware overwrite, on page 219
- ap name ipsla, on page 220
- ap name keepalive, on page 221
- ap name lan, on page 222
- ap name led, on page 223
- ap name led-brightness-level, on page 224
- ap name location, on page 225
- ap name mesh backhaul rate dot11abg, on page 226
- ap name mdsn-ap, on page 227
- ap name mesh backhaul rate dot11ac, on page 228
- ap name name mesh backhaul rate dot11ax , on page 229
- ap name name new-ap-name, on page 230
- ap name no, on page 231
- ap name mesh backhaul rate , on page 232
- ap name mesh backhaul rate dot11n, on page 233
- ap name mesh block-child, on page 234
- ap name mesh daisy-chaining, on page 235
- ap name mesh ethernet mode access, on page 236
- ap name mesh ethernet mode trunk, on page 237
- ap name mesh linktest, on page 238
- ap name mesh parent preferred, on page 239
- ap name mesh security psk provisioning delete, on page 240
- ap name mesh vlan-trunking native, on page 241
- ap name mode, on page 242
- ap name mode bridge, on page 244
- ap name monitor-mode, on page 245
- ap name monitor-mode dot11b, on page 246
- ap name management-mode meraki, on page 247
- ap name name, on page 248
- ap name network-diagnostics, on page 249
- ap name priority, on page 250
- ap name remote, on page 251
- ap name reset, on page 252
- ap name reset-button, on page 253
- ap name role, on page 254
- ap name sensor environment, on page 255

- ap name slot, on page 256
- ap name static-ip, on page 258
- ap name shutdown, on page 259
- ap name sniff, on page 260
- ap name tftp-downgrade, on page 261
- ap name urwb mode coordinator radio-off, on page 262
- ap name usb-module, on page 263
- ap name vlan-tag, on page 264
- ap name write tag-config , on page 265
- ap name-regex , on page 266
- ap neighborhood calendar-profile, on page 267
- ap neighborhood load-balance, on page 268
- ap packet-capture, on page 269
- ap packet-capture profile, on page 270
- ap packet-capture start, on page 271
- ap profile, on page 272
- ap regulatory activation apply, on page 273
- ap regulatory activation clear, on page 274
- ap regulatory activation file, on page 275
- ap remote-lan profile-name, on page 276
- ap remote-lan shutdown, on page 277
- ap remote-lan-policy policy-name, on page 278
- ap reset site-tag, on page 279
- ap sensor air-pressure, on page 280
- ap tag persistency enable, on page 281
- ap upgrade method https, on page 282
- ap upgrade staggered, on page 283
- ap upgrade staggered client-deauth, on page 284
- ap upgrade staggered iteration completion, on page 285
- ap upgrade staggered iteration error, on page 286
- ap upgrade staggered iteration timeout, on page 287
- ap tag-source-priority , on page 288
- ap tag-sources revalidate , on page 289
- ap triradio, on page 290
- ap vlan-tag, on page 291
- arp-caching, on page 292
- assisted-roaming, on page 293
- association-limit, on page 294
- attribute type, on page 295
- authentication-type, on page 296
- autoqos, on page 297
- avg-packet-size packetsize , on page 298
- avc sd-service, on page 299
- avoid label exhaustion error , on page 300
- awips, on page 301
- awips-syslog, on page 302

- backhaul (mesh), on page 303
- background-scanning (mesh), on page 304
- band-select client, on page 305
- band-select cycle, on page 306
- band-select expire, on page 307
- band-select probe-response, on page 308
- banner text, on page 309
- battery-state (mesh), on page 310
- boot system flash, on page 311
- bridge-group, on page 313
- bss-transition, on page 314
- bssid-stats bssid-stats frequency, on page 315
- bssid-neighbor-stats interval , on page 316
- bucket, on page 317
- cache timeout active value , on page 318
- cache timeout inactive value , on page 319
- call-snoop, on page 320
- calender-profile name, on page 321
- captive-bypass-portal, on page 322
- capwap-discovery, on page 323
- capwap aggregation, on page 324
- capwap backup, on page 325
- capwap window size , on page 326
- capwap udplite, on page 327
- ccn (mesh), on page 328
- ccx aironet-iesupport, on page 329
- cdp, on page 330
- central authentication, on page 331
- central dhcp, on page 332
- central switching, on page 333
- central-webauth, on page 334
- channel unii3-low-power-channels , on page 335
- chassis redundancy ha-interface, on page 336
- chassis redundancy ha-interface GigabitEthernet, on page 337
- chassis redundancy ha-interface shutdown, on page 338
- chassis redundancy keep-alive, on page 339
- chassis renumber, on page 340
- chassis priority, on page 341
- chassis transport, on page 342
- ciphersuite, on page 343
- cisco-dna grpc, on page 345
- class, on page 346
- classify, on page 349
- class-map, on page 350
- clear aaa counters servers radius, on page 352
- clear ap config, on page 353

- clear ap geolocation ranging site, on page 354
- clear ap meraki stats, on page 355
- clear ap sort statistics, on page 356
- clear chassis redundancy, on page 357
- clear ip nbar protocol-discovery wlan , on page 358
- clear mdns-sd statistics, on page 359
- clear platform condition all, on page 360
- clear platform hardware chassis active qfp feature wireless trace-buffer ingress, on page 361
- clear platform hardware chassis active qfp feature wireless trace-buffer punt-inject , on page 362
- clear platform software rif-mgr chassis active R0 clear-lmp-counters, on page 363
- clear platform software rif-mgr chassis standby R0 clear-lmp-counters, on page 364
- clear radius statistics, on page 365
- clear subscriber policy peer, on page 366
- clear wireless stats mobility, on page 367
- clear wireless stats mobility peer ip, on page 368
- clear wireless wps rogue ap, on page 369
- clear wireless wps rogue client, on page 370
- clear wireless wps rogue stats, on page 371
- clear wlan sort statistics, on page 372
- client-access (mesh), on page 373
- client association limit, on page 374
- client-aware-fra, on page 376
- cloud-services aws s3 profile, on page 377
- cloud-services aws cloudwatch profile, on page 378
- channel foreign, on page 379
- channel chan-width, on page 380
- channel psc, on page 381
- client-l2-vnid , on page 382
- client-steering, on page 383
- collect counter, on page 384
- collect wireless ap mac address (wireless), on page 385
- collect wireless client mac address (wireless), on page 386
- condition chan-width, on page 387
- connection-capability, on page 388
- consent activation-mode merge, on page 390
- console, on page 391
- console speed, on page 392
- controller, on page 393
- convergence, on page 394
- copy configuration download, on page 395
- copy configuration upload, on page 396
- core-dump kernel limit, on page 397
- core-dump kernel type, on page 398
- coverage, on page 399
- crypto key generate rsa, on page 400
- crypto pki trustpoint, on page 406

- crypto pki trust pool import terminal, on page 407
- crypto pki trustpool clean, on page 408
- cts inline-tagging, on page 409
- cts role-based enforcement, on page 410
- cts sgt, on page 411
- custom-page login device, on page 412
- default, on page 413
- daisychain-stp-redundancy, on page 416
- debug platform qos-acl-tcam, on page 417
- debug platform packet-trace, on page 418
- debug platform hardware chassis active qfp feature wireless datapath trace-buffer debug-level, on page 419
- debug platform hardware chassis active qfp feature wireless datapath trace-buffer ingress filtered-trace, on page 420
- debug platform hardware chassis active qfp feature wireless datapath trace-buffer ingress global-trace, on page 422
- debug platform hardware chassis active qfp feature wireless datapath trace-buffer punt-inject filtered-trace , on page 423
- debug platform hardware chassis active qfp feature wireless datapath trace-buffer punt-inject global-trace, on page 425
- debug qos-manager, on page 426
- debug wireless bundle client abort, on page 427
- debug wireless bundle client mac , on page 428
- debug wireless bundle client start, on page 429
- debug wireless bundle client stop-all collect, on page 430
- description, on page 431
- destination, on page 432
- device-role (IPv6 snooping), on page 433
- device-role (IPv6 nd inspection), on page 434
- device-tracking binding, on page 435
- device-tracking binding vlan, on page 436
- device-tracking policy, on page 437
- description word, on page 439
- destination-ports, on page 440
- dhcp broadcast, on page 441
- dhcp-server, on page 442
- dhcp-tlv-caching, on page 443
- dns-server (IPv6), on page 444
- dnscrypt, on page 445
- domain, on page 446
- domain-name (DHCP), on page 447
- dot11 24ghz | 5ghz data rate min, on page 448
- dot11 {24ghz | 5ghz | 6ghz} slot0 radio-profile, on page 449
- dot11 5ghz slot1 radio-profile, on page 450
- dot11 airtime-fairness, on page 451
- dot11be-profile, on page 452

- dot11 a-mpdu tx block-ack window-size, on page 453
- dot11ax, on page 454
- dot11ax bcast-probe-response, on page 455
- dot11ax bcast-probe-response time-interval, on page 456
- dot11ax fils-discovery, on page 457
- dot11ax multi-bssid-profile, on page 458
- dot11ax spatial-reuse obss-pd, on page 459
- dot11ax spatial-reuse obss-pd non-srg-max, on page 460
- dot11ax target-waketime, on page 461
- dot11ax twt-broadcast-support, on page 462
- dot11 {24ghz slot0 | 5ghz {slot1 | slot2} radio-profile, on page 463
- dot11bg 11g, on page 464
- dot11 5ghz reporting-interval , on page 465
- dot11 reporting-interval, on page 466
- dot1x system-auth-control, on page 467
- dot11-tlv-accounting, on page 469
- dscp, on page 470
- dual-mode-ap-deployment-mode, on page 471
- eap-method, on page 472
- eap profile, on page 474
- et-analytics, on page 475
- ethernet-vlan-transparent (mesh), on page 476
- ethernet-bridging (mesh), on page 477
- event identity-update, on page 478
- exclusionlist, on page 479
- exec-character-bits , on page 480
- exec time-out, on page 481
- exporter default-flow-exporter, on page 482
- fabric control-plane, on page 483
- factory-reset all, on page 484
- factory-reset all secure, on page 485
- fast-teardown, on page 486
- fallback-radio-shut, on page 487
- fips authorization-key, on page 488
- flex , on page 489
- flow exporter, on page 490
- flow monitor, on page 491
- flow record, on page 492
- full-sector-dfs (mesh), on page 493

24ghz-rf-policy default-dot11b-policy

To add required RF profile to RF tag and configure 802.11b policy within the default RF profile, use the **24ghz-rf-policy default-dot11b-policy** command in the global configuration mode. Use the **no** form of this command to disable the feature.

24ghz-rf-policy default-dot11b-policy

no 24ghz-rf-policy default-dot11b-policy

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Wireless RF tag configuration mode

Command History

Release	Modification
Cisco IOS XE 26.1.1	This command is introduced.

Example

This example shows how to add required RF profile to RF tag and configure 802.11b policy within the default RF profile in the global configuration mode:

```
Device# configure terminal
Device(config)# wireless tag
Device(config)# wireless tag rf default-rf-tag
Device(config-wireless-rf-tag)# 24ghz-rf-policy default-dot11b-policy
Device(config-wireless-rf-tag)# exit
```

3gpp-info

To configure a 802.11u 3rd Generation Partnership Project (3GPP) cellular network used by hotspots, use the **3gpp-info** command. To remove the network, use the **no** form of the command.

3gpp-info *country-code network-code*

Syntax Description

country-code	Mobile country code.
network-code	Mobile network code.

Command Default

None

Command Modes

Wireless ANQP Server Configuration (config-wireless-anqp-server)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Example

The following example shows how to configure a 802.11u 3GPP cellular network:

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# 3gpp-info us mcc
```

aaa accounting identity

To enable authentication, authorization, and accounting (AAA) for IEEE 802.1x, MAC authentication bypass (MAB), and web authentication sessions, use the **aaa accounting identity** command in global configuration mode. To disable IEEE 802.1x accounting, use the **no** form of this command.

aaa accounting identity {*name* | **default** } **start-stop** {**broadcast group** {*name* | **radius** | **tacacs+**} [**group** {*name* | **radius** | **tacacs+**} **. . .**] | **group** {*name* | **radius** | **tacacs+**} [**group** {*name* | **radius** | **tacacs+**} **. . .**] }
no aaa accounting identity {*name* | **default** }

Syntax Description

name	Name of a server group. This is optional when you enter it after the **broadcast group** and **group** keywords.
default	Uses the accounting methods that follow as the default list for accounting services.
start-stop	Sends a start accounting notice at the beginning of a process and a stop accounting notice at the end of a process. The start accounting record is sent in the background. The requested-user process begins regardless of whether or not the start accounting notice was received by the accounting server.
broadcast	Enables accounting records to be sent to multiple AAA servers and send accounting records to the first server in each group. If the first server is unavailable, the device uses the list of backup servers to identify the first server.
group	Specifies the server group to be used for accounting services. These are valid server group names: • *name* — Name of a server group. • **radius** — Lists of all RADIUS hosts. • **tacacs+** — Lists of all TACACS+ hosts. The **group** keyword is optional when you enter it after the **broadcast group** and **group** keywords. You can enter more than optional **group** keyword.
radius	(Optional) Enables RADIUS authorization.
tacacs+	(Optional) Enables TACACS+ accounting.

Command Default

AAA accounting is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

To enable AAA accounting identity, you need to enable policy mode. To enable policy mode, enter the **authentication display new-style** command in privileged EXEC mode.

This example shows how to configure IEEE 802.1x accounting identity:

```
Device# authentication display new-style

Please note that while you can revert to legacy style
configuration at any time unless you have explicitly
entered new-style configuration, the following caveats
should be carefully read and understood.

(1) If you save the config in this mode, it will be written
    to NVRAM in NEW-style config, and if you subsequently
    reload the router without reverting to legacy config and
    saving that, you will no longer be able to revert.

(2) In this and legacy mode, Webauth is not IPv6-capable. It
    will only become IPv6-capable once you have entered new-
    style config manually, or have reloaded with config saved
    in 'authentication display new' mode.

Device# configure terminal
Device(config)# aaa accounting identity default start-stop group radius
```

aaa accounting update periodic interval-in-minutes

To configure accounting update records intervals, use the **aaa accounting update periodic** command.

aaa accounting update periodic *interval-in-minutes* [**jitter maximum** *jitter-max-value*]

Syntax Description

periodic	Send accounting update records at regular intervals.
<1-71582>	Periodic intervals to send accounting update records(in minutes)
jitter	Set jitter parameters for periodic interval
maximum	Set maximum jitter value for periodic interval (in seconds)
<0-2147483>	Maximum jitter value for periodic interval(in seconds). Default is 300 seconds.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure the interval to five minutes at which the accounting records are updated:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# aaa accounting update periodic 5
```

aaa attribute list

To define an authentication, authorization, and accounting (AAA) attribute list locally on a device, use the **aaa attribute list** command in either the global configuration mode or IKEv2 authorization policy configuration mode. To remove the AAA attribute list, use the **no** form of this command.

aaa attribute list *list-name*

Syntax Description

Keywords and Variables	Description
list-name	Name of an attribute list.

Command Default

A local attribute list is not defined.

Command Modes

Global Configuration (config)

IKEv2 authorization policy configuration (config-ikev2-author-policy)

Command History

Release	Modification
Cisco IOS XE 17.12.1	This command was introduced in a release earlier than Cisco IOS XE 17.12.1.

Usage Guidelines

There is no limit to the number of lists that can be defined (except for NVRAM storage limits). Use this command to refer to an AAA attribute list. This list must be defined in global configuration mode. Among the AAA attributes, the list can have the **interface-config** attribute that is used to apply interface configuration mode commands on the virtual access interface associated with the session.

The example shows how to apply the AAA attribute list **attr-list1** to the IKEv2 authorization policy **pol1** to dynamically configure interface settings like MTU and tunnel key.

```
!
aaa attribute list attr-list1
attribute type interface-config "ip mtu 1100"
attribute type interface-config "tunnel key 10"
!
!
crypto ikev2 authorization policy pol1
 aaa attribute list attr-list1
!
```

aaa authentication dot1x

To specify the authentication, authorization, and accounting (AAA) method to use on ports complying with the IEEE 802.1x authentication, use the **aaa authentication dot1x** command in global configuration mode . To disable authentication, use the **no** form of this command.

aaa authentication dot1x {**default**} *method1*
no aaa authentication dot1x {**default**} *method1*

Syntax Description

default	The default method when a user logs in. Use the listed authentication method that follows this argument.
method1	Specifies the server authentication. Enter the **group radius** keywords to use the list of all RADIUS servers for authentication. **Note** Though other keywords are visible in the command-line help strings, only the **default** and **group radius** keywords are supported.

Command Default

No authentication is performed.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

The **method** argument identifies the method that the authentication algorithm tries in the specified sequence to validate the password provided by the client. The only method that is IEEE 802.1x-compliant is the **group radius** method, in which the client data is validated against a RADIUS authentication server.

If you specify **group radius**, you must configure the RADIUS server by entering the **radius-server host** global configuration command.

Use the **show running-config** privileged EXEC command to display the configured lists of authentication methods.

This example shows how to enable AAA and how to create an IEEE 802.1x-compliant authentication list. This authentication first tries to contact a RADIUS server. If this action returns an error, the user is not allowed access to the network.

```
Device(config)# aaa new-model
Device(config)# aaa authentication dot1x default group radius
```

aaa authentication login

To set authentication, authorization, and accounting (AAA) at login, use the **aaa authentication login** command in global configuration mode.

aaa authentication login *authentication-list-name* {**group** }*group-name*

Syntax Description

authentication-list-name	Character string used to name the list of authentication methods activated when a user logs in.
group	Uses a subset of RADIUS servers for authentication as defined by the server group **group-name**.
group-name	Server group name.

Command Default

None

Command Modes

Global Configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Examples

The following example shows how to set an authentication method list named **local_webauth** to the group type named **local** in local web authentication:

```
Device(config)# aaa authentication login local_webauth local
```

The following example shows how to set an authentication method to RADIUS server group in local web authentication:

```
Device(config)# aaa authentication login webauth_radius group ISE_group
```

aaa authorization

To set the parameters that restrict user access to a network, use the **aaa authorization** command in global configuration mode. To remove the parameters, use the **no** form of this command.

aaa authorization { **auth-proxy** | **cache** | **commands** *level* | **config-commands** | **configuration** | **console** | **credential-download** | **exec** | **multicast** | **network** | **onep** | **policy-if** | **prepaid** | **radius-proxy** | **reverse-access** | **subscriber-service** | **template**} {**default** | *list_name* } [*method1* [*method2* . . .]]

Syntax Description

auth-proxy	Runs authorization for authentication proxy services.
cache	Configures the authentication, authorization, and accounting (AAA) server.
commands	Runs authorization for all commands at the specified privilege level.
level	Specific command level that should be authorized. Valid entries are 0 through 15.
config-commands	Runs authorization to determine whether commands entered in configuration mode are authorized.
configuration	Downloads the configuration from the AAA server.
console	Enables the console authorization for the AAA server.
credential-download	Downloads EAP credential from Local/RADIUS/LDAP.
exec	Enables the console authorization for the AAA server.
multicast	Downloads the multicast configuration from the AAA server.
network	Runs authorization for all network-related service requests, including Serial Line Internet Protocol (SLIP), PPP, PPP Network Control Programs (NCPs), and AppleTalk Remote Access (ARA).
onep	Runs authorization for the ONEP service.
reverse-access	Runs authorization for reverse access connections, such as reverse Telnet.
template	Enables template authorization for the AAA server.
default	Uses the listed authorization methods that follow this keyword as the default list of methods for authorization.
list_name	Character string used to name the list of authorization methods.
method1 [*method2...*]	(Optional) An authorization method or multiple authorization methods to be used for authorization. A method may be any one of the keywords listed in the table below.

Command Default

Authorization is disabled for all actions (equivalent to the method keyword **none**).

Command Modes Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines Use the **aaa authorization** command to enable authorization and to create named methods lists, which define authorization methods that can be used when a user accesses the specified function. Method lists for authorization define the ways in which authorization will be performed and the sequence in which these methods will be performed. A method list is a named list that describes the authorization methods (such as RADIUS or TACACS+) that must be used in sequence. Method lists enable you to designate one or more security protocols to be used for authorization, which ensures a backup system in case the initial method fails. Cisco IOS software uses the first method listed to authorize users for specific network services; if that method fails to respond, the Cisco IOS software selects the next method listed in the method list. This process continues until there is successful communication with a listed authorization method, or until all the defined methods are exhausted.



Note The Cisco IOS software attempts authorization with the next listed method only when there is no response from the previous method. If authorization fails at any point in this cycle--meaning that the security server or the local username database responds by denying the user services--the authorization process stops and no other authorization methods are attempted.

If the **aaa authorization** command for a particular authorization type is issued without a specified named method list, the default method list is automatically applied to all interfaces or lines (where this authorization type applies) except those that have a named method list explicitly defined. (A defined method list overrides the default method list.) If no default method list is defined, then no authorization takes place. The default authorization method list must be used to perform outbound authorization, such as authorizing the download of IP pools from the RADIUS server.

Use the **aaa authorization** command to create a list by entering the values for the *list-name* and the *method* arguments, where *list-name* is any character string used to name this list (excluding all method names) and *method* identifies the list of authorization methods tried in the given sequence.



Note In the table that follows, the **group***group-name*, **group ldap**, **group radius**, and **group tacacs+** methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius server** and **tacacs server** commands to configure the host servers. Use the **aaa group server radius**, **aaa group server ldap**, and **aaa group server tacacs+** commands to create a named group of servers.

This table describes the method keywords.

Table 1: aaa authorization Methods

Keyword	Description
cache *group-name*	Uses a cache server group for authorization.

Keyword	Description
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the **server group** *group-name* command.
group ldap	Uses the list of all Lightweight Directory Access Protocol (LDAP) servers for authentication.
group radius	Uses the list of all RADIUS servers for authentication as defined by the **aaa group server radius** command.
grouptacacs+	Uses the list of all TACACS+ servers for authentication as defined by the **aaa group server tacacs+** command.
if-authenticated	Allows the user to access the requested function if the user is authenticated. **Note** The **if-authenticated** method is a terminating method. Therefore, if it is listed as a method, any methods listed after it will never be evaluated.
local	Uses the local database for authorization.
none	Indicates that no authorization is performed.

Cisco IOS software supports the following methods for authorization:

- Cache Server Groups—The router consults its cache server groups to authorize specific rights for users.
- If-Authenticated—The user is allowed to access the requested function provided the user has been authenticated successfully.
- Local—The router or access server consults its local database, as defined by the **username** command, to authorize specific rights for users. Only a limited set of functions can be controlled through the local database.
- None—The network access server does not request authorization information; authorization is not performed over this line or interface.
- RADIUS—The network access server requests authorization information from the RADIUS security server group. RADIUS authorization defines specific rights for users by associating attributes, which are stored in a database on the RADIUS server, with the appropriate user.
- TACACS+—The network access server exchanges authorization information with the TACACS+ security daemon. TACACS+ authorization defines specific rights for users by associating attribute-value (AV) pairs, which are stored in a database on the TACACS+ security server, with the appropriate user.

Method lists are specific to the type of authorization being requested. AAA supports five different types of authorization:

- Commands—Applies to the EXEC mode commands a user issues. Command authorization attempts authorization for all EXEC mode commands, including global configuration commands, associated with a specific privilege level.
- EXEC—Applies to the attributes associated with a user EXEC terminal session.
- Network—Applies to network connections. The network connections can include a PPP, SLIP, or ARA connection.



Note You must configure the **aaa authorization config-commands** command to authorize global configuration commands, including EXEC commands prepended by the **do** command.

- Reverse Access—Applies to reverse Telnet sessions.
- Configuration—Applies to the configuration downloaded from the AAA server.

When you create a named method list, you are defining a particular list of authorization methods for the indicated authorization type.

Once defined, the method lists must be applied to specific lines or interfaces before any of the defined methods are performed.

The authorization command causes a request packet containing a series of AV pairs to be sent to the RADIUS or TACACS daemon as part of the authorization process. The daemon can do one of the following:

- Accept the request as is.
- Make changes to the request.
- Refuse the request and authorization.

For a list of supported RADIUS attributes, see the module RADIUS Attributes. For a list of supported TACACS+ AV pairs, see the module TACACS+ Attribute-Value Pairs.



Note Five commands are associated with privilege level 0: **disable**, **enable**, **exit**, **help**, and **logout**. If you configure AAA authorization for a privilege level greater than 0, these five commands will not be included in the privilege level command set.

The following example shows how to define the network authorization method list named mygroup, which specifies that RADIUS authorization will be used on serial lines using PPP. If the RADIUS server fails to respond, local network authorization will be performed.

```
Device(config)#  aaa authorization network mygroup group radius local
```

aaa authorization credential download default

To set an authorization method list to use local credentials, use the **aaa authorization credential download default** command in global configuration mode.

aaa authorization credential download default *group-name*

Syntax Description

group-name	Server group name.

Command Default

None

Command Modes

Global Configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

The following example shows how to set an authorization method list to use local credentials:

```
Device(config)# aaa authorization credential-download default local
```

aaa authorization credential-download MY-METHOD-LIST group MY-SERVER-GROUP

To configure the authorization method list with the named RADIUS server group, use the **aaa authorization credential-download MY-METHOD-LIST group** *My-server-group* command. This command has a limit of 14 lines.

aaa authorization credential-download MY-METHOD-LIST group { *My-server-group* | *ldap* | *radius* | *tacacs+* }

Syntax Description

My-Server-Group	Specifies the server group name.
ldap	Specifies the list of all LDAP hosts.
radius	Specifies the list of all RADIUS hosts.
tacacs+	Specifies the list of all TACACS+ hosts.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.18.1	This command was introduced.

Examples

The following example shows how to configure the authorization method list with the named RADIUS server group:

```
Device# configure terminal
Device(config)# aaa authorization credential-download MY-METHOD-LIST group MY-SERVER-GROUP
```

aaa group server ldap

To configure a AAA server group, use the **aaa group server ldap** command.

aaa group server ldap *group-name*

Command Default None

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.1	This command was introduced.

This example shows how to configure a AAA server group:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# aaa new-model
Device(config)# aaa group server ldap name1
Device(config-ldap-sg)# server server1
Device(config-ldap-sg)# exit
```

aaa group server radius

To group different RADIUS server hosts into distinct lists and distinct methods, use the **aaa group server radius** command in global configuration mode.

aaa group server radius *group-name*

Syntax Description

group-name	Character string used to name the group of servers.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

The authentication, authorization, and accounting (AAA) server-group feature introduces a way to group existing server hosts. The feature enables you to select a subset of the configured server hosts and use them for a particular service.

A group server is a list of server hosts of a particular type. Currently supported server host types are RADIUS server hosts. A group server is used in conjunction with a global server host list. The group server lists the IP addresses of the selected server hosts.

The following example shows how to configure an AAA group server named **ISE_Group** that comprises three member servers:

```
Device(config)# aaa group server radius ISE_Group
```

aaa local authentication default authorization

To configure local authentication method list, use the **aaa local authentication default authorization** command.

aaa local authentication default authorization [*method-list-name* | **default**]

Syntax Description

method-list-name	Name of the method list.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure local authentication method list to the default list:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# aaa local authentication default authorization default
```

aaa new-model

To enable the authentication, authorization, and accounting (AAA) access control model, issue the **aaa new-model** command in global configuration mode. To disable the AAA access control model, use the **no** form of this command.

aaa new-model
no aaa new-model

Syntax Description

This command has no arguments or keywords.

Command Default

AAA is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

This command enables the AAA access control system.

If the **login local** command is configured for a virtual terminal line (VTY), and the **aaa new-model** command is removed, you must reload the device to get the default configuration or the **login** command. If the device is not reloaded, the device defaults to the **login local** command under the VTY.

Note We do not recommend removing the **aaa new-model** command.

The following example shows this restriction:

```
Device(config)# aaa new-model
Device(config)# line vty 0 15
Device(config-line)# login local
Device(config-line)# exit
Device(config)# no aaa new-model
Device(config)# exit
Device# show running-config | b line vty

line vty 0 4
 login local  !<=== Login local instead of "login"
line vty 5 15
 login local
!
```

Examples

The following example initializes AAA:

```
Device(config)# aaa new-model
Device(config)#
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.
aaa authentication arap	Enables an AAA authentication method for ARAP using TACACS+.
aaa authentication enable default	Enables AAA authentication to determine if a user can access the privileged command level.
aaa authentication login	Sets AAA authentication at login.
aaa authentication ppp	Specifies one or more AAA authentication method for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict user access to a network.

aaa server radius dynamic-author

To configure a device as an authentication, authorization, and accounting (AAA) server to facilitate interaction with an external policy server, use the **aaa server radius dynamic-author**command in global configuration mode. To remove this configuration, use the **no** form of this command.

aaa server radius dynamic-author
no aaa server radius dynamic-author

Syntax Description

This command has no arguments or keywords.

Command Default

The device will not function as a server when interacting with external policy servers.

Command Modes

Global configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.4	This command was integrated into Cisco IOS Release 12.4.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.
12.2(5)SXI	This command was integrated into Cisco IOS Release 12.2(5)SXI.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.
	This command was introduced.

Usage Guidelines

Dynamic authorization allows an external policy server to dynamically send updates to a device. Once the **aaa server radius dynamic-author** command is configured, dynamic authorization local server configuration mode is entered. Once in this mode, the RADIUS application commands can be configured.

Dynamic Authorization for the Intelligent Services Gateway (ISG)

ISG works with external devices, referred to as policy servers, that store per-subscriber and per-service information. ISG supports two models of interaction between the ISG device and external policy servers: initial authorization and dynamic authorization.

The dynamic authorization model allows an external policy server to dynamically send policies to the ISG. These operations can be initiated in-band by subscribers (through service selection) or through the actions of an administrator, or applications can change policies on the basis of an algorithm (for example, change session quality of service (QoS) at a certain time of day). This model is facilitated by the Change of Authorization (CoA) RADIUS extension. CoA introduced peer-to-peer capability to RADIUS, enabling ISG and the external policy server each to act as a RADIUS client and server.

Examples

The following example configures the ISG to act as a AAA server when interacting with the client at IP address 10.12.12.12:

```
aaa server radius dynamic-author
```

```
client 10.12.12.12 key cisco
message-authenticator ignore
```

Related Commands

Command	Description
auth-type (ISG)	Specifies the server authorization type.
client	Specifies a RADIUS client from which a device will accept CoA and disconnect requests.
default	Sets a RADIUS application command to its default.
domain	Specifies username domain options.
ignore	Overrides a behavior to ignore certain paremeters.
port	Specifies a port on which local RADIUS server listens.
server-key	Specifies the encryption key shared with RADIUS clients.

aaa session-id

To specify whether the same session ID will be used for each authentication, authorization, and accounting (AAA) accounting service type within a call or whether a different session ID will be assigned to each accounting service type, use the **aaa session-id** command in global configuration mode. To restore the default behavior after the **unique** keyword is enabled, use the **no** form of this command.

aaa session-id [**common** | **unique**]
no aaa session-id [**unique**]

Syntax Description

common	(Optional) Ensures that all session identification (ID) information that is sent out for a given call will be made identical. The default behavior is **common**.
unique	(Optional) Ensures that only the corresponding service access-requests and accounting-requests will maintain a common session ID. Accounting-requests for each service will have a different session ID.

Command Default

The **common** keyword is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
	This command was integrated in Cisco IOS XE 16.12.1.

Usage Guidelines

The **common** keyword behavior allows the first session ID request of the call to be stored in a common database; all proceeding session ID requests will retrieve the value of the first session ID. Because a common session ID is the default behavior, this functionality is written to the system configuration after the **aaa new-model** command is configured.



Note The router configuration will always have either the **aaa session-id common** or the **aaa session-id unique** command enabled; it is not possible to have neither of the two enabled. Thus, the **no aaa session-id unique** command will revert to the default functionality, but the **no aaa session-id common** command will not have any effect because it is the default functionality.

The **unique** keyword behavior assigns a different session ID for each accounting type (Auth-Proxy, Exec, Network, Command, System, Connection, and Resource) during a call. To specify this behavior, the unique

keyword must be specified. The session ID may be included in RADIUS access requests by configuring the **radius-server attribute 44 include-in-access-req**command. The session ID in the access-request will be the same as the session ID in the accounting request for the same service; all other services will provide unique session IDs for the same call.

Examples

The following example shows how to configure unique session IDs:

```
aaa new-model
aaa authentication ppp default group radius
radius-server host 10.100.1.34
radius-server attribute 44 include-in-access-req
aaa session-id unique
```

Related Commands

Command	Description
aaa new model	Enables AAA.
radius-server attribute 44 include-in-access-req	Sends RADIUS attribute 44 (Accounting Session ID) in access request packets before user authentication (including requests for preauthentication).

access-session wireless cui-enable

To enable Chargeable User Identity (CUI) attribute in the authentication and accounting messages sent to a AAA server, use the **access-session wireless cui-enable** command. To disable the CUI attribute in the authentication and accounting messages sent to a AAA server, use the **no** form of this command.

access-session wireless cui-enable

no access-session wireless cui-enable

Syntax Description

This command has no keywords or arguments.

Command Default

CUI is not enabled.

Command Modes

Global Configuration (config)

Command History

Release	Modification
Cisco IOS XE Cupertino 17.9.1	This command was introduced.

Usage Guidelines

Setting CUI attribute is applicable only for 802.1x clients.

Examples

The following example shows how to enable the CUI attribute in the authentication and accounting messages sent to a AAA server:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# access-session wireless cui-enable
```

aaa-override

To enable AAA override, use the **aaa-override** command. To disable AAA override, use the **no** form of this command.

aaa-override

no aaa-override

Syntax Description

This command has no keywords or arguments.

Command Default

AAA is disabled by default.

Command Modes

Wireless policy configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

This example shows how to enable AAA:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy policy-test
Device(config-wireless-policy)# aaa-override
```

aaa-override vlan fallback

To allow fallback to policy profile VLAN when the overridden VLAN is not available, use the **aaa-override vlan fallback** command, in the wireless policy configuration mode. To disable fallback to policy profile VLAN, use the **no** form of this command.

aaa-override vlan fallback

no aaa-override vlan fallback

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Wireless policy configuration mode

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.6.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows you how to allow fallback to policy profile VLAN when the overridden VLAN is not available:

```
Device# configure terminal
Device(config)# wireless profile policy defalt-policy-profile
Device(config-wireless-policy)# aaa-override vlan fallback
```

aaa-policy

To map a AAA policy in a WLAN policy profile, use the **aaa-policy** command.

aaa-policy *aaa-policy-name*

Syntax Description

aaa-policy-name	Name of the AAA policy.

Command Default

None

Command Modes

config-wireless-policy

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to map a AAA policy in a WLAN policy profile:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy policy-name
Device(config-wireless-policy)# aaa-policy aaa-policy-name
```

aaa-realm enable

To enable AAA RADUIS selection by realm, use the **aaa-realm enable** command.

aaa-realm enable

Command Default None

Command Modes config-aaa-policy

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to enable AAA RADIUS section by realm:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless aaa policy aaa-profile-name
Device (config-aaa-policy)#  aaa-realm enable
```

absolute-timer

To enable an absolute timeout for subscriber sessions, use the **absolute-timer** command in service template configuration mode. To disable the timer, use the **no** form of this command.

absolute-timer *minutes*
no absolute-timer

Syntax Description

minutes	Maximum session duration, in minutes. Range: 1 to 65535. Default: 0, which disables the timer.

Command Default

Disabled (the absolute timeout is 0).

Command Modes

Service template configuration (config-service-template)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was introduced.

Usage Guidelines

Use the **absolute-timer** command to limit the number of minutes that a subscriber session can remain active. After this timer expires, a session must repeat the process of establishing its connection as if it were a new request.

Examples

The following example shows how to set the absolute timeout to 15 minutes in the service template named SVC_3:

```
service-template SVC_3
 description sample
 access-group ACL_2
 vlan 113
 inactivity-timer 15
 absolute-timer 15
```

Related Commands

Command	Description
event absolute-timeout	Specifies the type of event that triggers actions in a control policy if conditions are met.
inactivity-timer	Enables an inactivity timeout for subscriber sessions.
show service-template	Displays configuration information for service templates.

access-list

To add an access list entry, use the **access-list** command.

access-list {*1-99* *100-199* *1300-1999* *2000-2699*} [*sequence-number*] {**deny** | **permit**} {*hostname-or-ip-addr* [*wildcard-bits* | **log**] | **any** [**log**] | **host** *hostname-or-ip-addr* **log**} | {**remark** [*line*]}

Syntax Description

1-99	Configures IP standard access list.
100-199	Configures IP extended access list.
1300-1999	Configures IP standard access list (expanded range).
2000-2699	Configures IP extended access list (expanded range).
sequence-number	Sequence number of the ACL entry. Valid range is 1 to 2147483647.
deny	Configures packets to be rejected.
permit	Configures packets to be forwarded.
hostname-or-ip-addr	Hostname or the IP address to match.
wildcard-bits	Wildcard bits to match the IP address.
log	Configures log matches against this entry.
any	Any source host.
host	A single host address.
remark	Configures ACL entry comment.
line	The ACL entry comment.

Command Default

None

Command Modes

Global Config

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to add an access list entry:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# access-list 1 permit any
```

access-key (cloudwatch)

To configure AWS CloudWatch access credentials, use the **access-key** command. To remove AWS CloudWatch access credentials, use the **no** form of the command.

access-key key-id *iam-id* **secret-key** *secret-key*

no access-key key-id *iam-id* **secret-key** *secret-key*

Syntax Description

iam-id	AWS access key ID.
secret-key	Password for managing the AWS access key.

Command Default

Access key is not configured.

Command Modes

CloudWatch Profile Configuration (config-cloudwatch-profile)#

Command History

Release	Modification
Cisco IOS XE 17.13.1	This command was introduced.

Examples

The following example shows how to configure AWS CloudWatch access credentials.

```
Device# configure terminal
Device(config)# cloud-services aws cloud-watch profile test-profile
Device(config-cloudwatch-profile)# access-key iam-key-id awskey secret-key 0 xxxxx
```

access-list acl-ace-limit

To set the maximum configurable ace limit for all ACLs, use the **access-list acl-ace-limit** command.

access-list acl-ace-limit *max-ace-limit*

Syntax Description

max-ace-limit	Maximum number of ace limit for all ACLs. Valid range is 1 to 4294967295.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to set the maximum configurable ace limit for all ACLs to 100:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# access-list acl-ace-limit 100
```

accounting-list

To configure RADIUS accounting servers on a WLAN policy profile, use the **accounting-list** command. To disable RADIUS server accounting, use the **no** form of this command.

accounting-list *radius-server-acct*
no accounting-list

Syntax Description

radius-server-acct	Accounting RADIUS server name.

Command Default

RADIUS server accounting is disabled by default.

Command Modes

WLAN policy configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

This example shows how to configure RADIUS server accounting on a WLAN policy profile:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy rr-xyz-policy-1
Device(config-wireless-policy)# accounting-list test
Device(config-wireless-policy)# no shutdown
```

This example shows how to disable RADIUS server accounting on a WLAN policy profile:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy rr-xyz-policy-1
Device(config-wireless-policy)# no accounting-list test
Device(config-wireless-policy)# no shutdown
```

acl-policy

To configure an access control list (ACL) policy, use the **acl-policy** command.

acl-policy *acl-policy-name*

Syntax Description

acl-policy-name	Name of the ACL policy.

Command Default

None

Command Modes

config-wireless-flex-profile

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure an ACL policy name:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile flex default-flex-profile
Device(config-wireless-flex-profile)# acl-policy my-acl-policy
```

active testing radio-selection always

To configure and enable the radio to be always available for WAT, use the **active testing radio-selection always** command in the radio profile configuration mode.

active testing radio-selection always

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Radio profile configuration mode

Command History

Release	Modification
Cisco IOS XE Cupertino 17.18.2	This command is introduced.

Examples

This example shows how to configure and enable the radio to be always available for WAT in the radio profile configuration mode:

```
Device# configure terminal
Device(config)# wireless profile radio RADIO_PROFILE_NAME
Device(config-wireless-radio-profile)# active testing radio-selection always
Device(config-wireless-radio-profile)# end
```

action power-saving-mode power-profile

To map a specific power profile to a specific calendar profile and to map the power saving mode action for the calendar profile, use the **action power-saving-mode power-profile** command. Use the **no** form of this command to disable the command.

action power-saving-mode power-profile *power-profile-name*

[no] action power-saving-mode power-profile *power-profile-name*

Syntax Description

power-profile-name	Specifies the name of the power profile.

Command Default

None

Command Modes

AP calendar profile configuration mode.

Command History

Release	Modification
Cisco IOS XE Cupertino 17.8.1	This command was introduced.

Example

The following example shows how to map a specific power profile to a specific calendar profile and to map the power saving mode action for the calendar profile:

```
Device(config)# ap profile ap-profile-name
Device(config-ap-profile)# calendar-profile ap-calendar-profile
Device(config-ap-profile-calendar)# action power-saving-mode power-profile power-profile1
```

address

To specify the IP address of the Rivest, Shamir, and Adelman (RSA) public key of the remote peer that you will manually configure in the keyring, use the **address** command inrsa-pubkey configuration mode. To remove the IP address, use the **no** form of this command.

address *ip-address*
no address *ip-address*

Syntax Description

ip-address	IP address of the remote peer.

Command Default

No default behavior or values

Command Modes

Rsa-pubkey configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

Before you can use this command, you must enter the **rsa-pubkey** command in the crypto keyring mode.

Examples

The following example specifies the RSA public key of an IP Security (IPSec) peer:

```
Router(config)# crypto keyring vpnkeyring
Router(conf-keyring)# rsa-pubkey name host.vpn.com
Router(config-pubkey-key)# address 10.5.5.1
Router(config-pubkey)# key-string
Router(config-pubkey)# 00302017 4A7D385B 1234EF29 335FC973
Router(config-pubkey)# 2DD50A37 C4F4B0FD 9DADE748 429618D5
Router(config-pubkey)# 18242BA3 2EDFBDD3 4296142A DDF7D3D8
Router(config-pubkey)# 08407685 2F2190A0 0B43F1BD 9A8A26DB
Router(config-pubkey)# 07953829 791FCDE9 A98420F0 6A82045B
Router(config-pubkey)# 90288A26 DBC64468 7789F76E EE21
Router(config-pubkey)# quit
Router(config-pubkey-key)# exit
Router(conf-keyring)# exit
```

Related Commands

Command	Description
crypto keyring	Defines a crypto keyring to be used during IKE authentication.

Command	Description
key-string	Specifies the RSA public key of a remote peer.
rsa-pubkey	Defines the RSA manual key to be used for encryption or signatures during IKE authentication.

address

To configure Software-Defined Application Visibility and Control (SD-AVC) controller IP address, use the **address** command. To remove the SD-AVC controller IP address, use the **no** form of this command.

address *ipv4-address*

no address

Syntax Description

ipv4-address	IPv4 address of the SD-AVC controller.

Command Default

Controller IP address is not configured.

Command Modes

SD Service Controller Configuration (config-sd-service-controller)

Command History

Release	Modification
Cisco IOS XE Cupertino 17.7.1	This command was introduced.

Usage Guidelines

Supports only IPv4 address.

Examples

The following example shows how to configure SD-AVC controller IP address:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
VM1(config)# avc sd-service
Device(config-sd-service)# controller
Device(config-sd-service-controller)# address 209.165.201.0
```

address-family ipv4

To set an IPv4 address family, use the **address-family ipv4** command. To remove the behavior of this command, use the **no** form of this command.

address-family ipv4

no address-family ipv4

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

VRF configuration (config-vrf)

Command History

Release	Modification
Cisco IOS XE 17.13.1	This command was introduced.

Examples

This example shows how to set an IPv4 address family:

```
Device# configure terminal
Device(config)# vrf definition mcast
Device(config-vrf)# address-family ipv4
Device(config-vrf)# exit-address-family
```

address prefix

To specify an address prefix for address assignment, use the **address prefix** command in interface configuration mode. To remove the address prefix, use the **no** form of this command.

address prefix ipv6-prefix [**lifetime** {**valid-lifetime preferred-lifetime** | **infinite**}]
no address prefix

Syntax Description

ipv6-prefix	IPv6 address prefix.
lifetime {valid-lifetime preferred-lifetime | infinite}]	(Optional) Specifies a time interval (in seconds) that an IPv6 address prefix remains in the valid state. If the **infinite** keyword is specified, the time interval does not expire.

Command Default

No IPv6 address prefix is assigned.

Command Modes

DHCP pool configuration (config-dhcpv6)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

You can use the **address prefix** command to configure one or several address prefixes in an IPv6 DHCP pool configuration. Each time the IPv6 DHCP address pool is used, an address will be allocated from each of the address prefixes associated with the IPv6 DHCP pool.

Examples

The following example shows how to configure a pool called engineering with an IPv6 address prefix:

```
Router(config)# ipv6 dhcp pool engineering
Router(config-dhcpv6)# address prefix 2001:1000::0/64 lifetime infinite
```

Related Commands

Command	Description
ipv6 dhcp pool	Configures a DHCPv6 server configuration information pool and enters DHCPv6 pool configuration mode.

advice-charge

To configure advice of charge for using the service set identifier (SSID) of each of the Network Access Identifier (NAI) realm, use the **advice-charge** command. To remove the advice of charge, use the **no** form of this command.

advice-charge {**data** | **time** | **time-and-data** | **unlimited**}

Syntax Description

data	Specifies charges based on the data volume.
time	Specifies charges based on time.
time-and-data	Specifies charges based on time and data volume.
unlimited	Specifies charges for unlimited access.

Command Default

Advice of charge is not configured.

Command Modes

Wireless ANQP Server Configuration (config-wireless-anqp-server)

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.3.1	This command was introduced.

Example

The following example shows how to configure advice of charge for using the SSID of each NAI realm:

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# advice-charge unlimited
```

advertise ap-name

To configure inclusion of AP hostname in beacon and probe response, use the **advertise ap-name** command.

advertise ap-name

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

WLAN configuration (config-wlan)

Command History

Release	Modification
Cisco IOS XE 17.18.2	This command was introduced.

Examples

The following example shows you how to configure inclusion of AP hostname in beacon and probe response:

```
Device(config)# wlan wlan-prof-name wlan-id ssid-name
Device(config-wlan)# advertise ap-name
```

airtime-fairness mode

Note Cisco Air Time Fairness (ATF) must be enabled on 2.4- or 5-GHz radios separately.

To configure airtime-fairness in different modes, use the **airtime-fairness mode** command.

airtime-fairness mode { **enforce-policy** | **monitor** }

Syntax Description

enforce-policy	This mode signifies that the ATF is operational.
monitor	This mode gathers information about air time and reports air time usage.

Command Default

None

Command Modes

RF Profile configuration (config-rf-profile)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

This example shows how to configure air time fairness in different modes:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap dot11 24ghz rf-profile rfprof24_1
Device(config-rf-profile)# airtime-fairness mode enforce-policy
Device(config-rf-profile)# airtime-fairness optimization
Device(config-rf-profile)# end
```

allow at-least min-number at-most max-number

To limit the number of multicast RAs per device per throttle period in an RA throttler policy, use the **allow at-least** *min-number* **at-most** *max-number* command.

allow at-least *min-number* **at-most** {*max-number* | **no-limit**}

Syntax Description

at-least *min-number*	Enter the minimum guaranteed number of multicast RAs per router before throttling can be enforced. Valid range is 0 to 32.
at-most *max-number*	Enter the maximum number of multicast RAs from router by which throttling is enforced. Valid range is 0 to 256.
at-most no-limit	No upper bound at the router level.

Command Default

None

Command Modes

config-nd-ra-throttle

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to limit the number of multicast RAs per device per throttle period in an RA throttler policy:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ipv6 nd ra-throttler policy ra-throttler-policy-name
Device(config-nd-ra-throttle)# allow at-least 5 at-most 10
```

amsdu (mesh)

To configure backhaul aggregated MAC service data unit (A-MSDU) for a mesh AP profile, use the **amsdu** command.

amsdu

Syntax Description

This command has no keywords or arguments.

Command Default

amsdu is enabled.

Command Modes

config-wireless-mesh-profile

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Example

The following example shows how to configure A-MSDU for a mesh AP profile:

```
Device # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device (config)# wireless profile mesh mesh-profile
Device (config-wireless-mesh-profile)# amsdu
```

anqp

To configure the Generic Advertisement Service (GAS) or the Access Network Query Protocol (ANQP) protocol settings, use the **anqp** command. To remove the protocol settings, use the **no** form of the command .

anqp {**fragmentation-threshold** *fragmentation-threshold* | **gas-timeout** *gas-timeout*}

Syntax Description

fragmentation-threshold	ANQP reply fragmentation threshold, in bytes. Valid range is from 16-1462.
gas-timeout	GAS request timeout, in milliseconds. Valid range is from 100-10000.

Command Default

None

Command Modes

Wireless ANQP Server Configuration (config-wireless-anqp-server)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Example

The following example shows how to configure GAS request timeout:

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# anqp gas-timeout 100
```

anqp-domain-id

To configure the Hotspot 2.0 Access Network Query Protocol (ANQP) domain identifier, use the **anqp-domain-id** command. To remove the domain identifier, use the **no** form of the command .

anqp-domain-id *domain-id*

Syntax Description

domain-id	ANQP domain ID. The range is from 0 to 65535.

Command Default

None

Command Modes

Wireless ANQP Server Configuration (config-wireless-anqp-server)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Example

The following example shows how to configure the Hotspot 2.0 ANQP domain identifier:

```
Device(config)#wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# anqp-domain-id 100
```

antenna beam-selection

To configure beam selection of the antenna, use the **antenna beam-selection** command, in the wireless radio profile configuration mode. Use the **no** form of this command to disable the feature.

antenna beam-selection { **narrow tilt** { **10** | **20** } | **wide** }

Syntax Description

narrow tilt { **10** | **20** }	Configures the tilt degrees for narrow beam selection. You can configure it for 10 degrees or 20 degrees tilt.
10 | **20**	Configures the tilt degree of the narrow beam selection for 10 degrees or 20 degrees.
wide	Configures the wide beam selection.

Command Default

None

Command Modes

Wireless radio profile configuration mode

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.6.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows how to configure the beam selection of the antenna:

```
Device# configure terminal
Device(config)# wireless profile radio radio-profile-name
Device(config-wireless-profile)# antenna beam-selection narrow tilt 10
```

antenna count

To configure the number of antennas to be enabled under a radio profile, use the **antenna count** command, in the radio profile configuration mode. To disable the number of antennas configured, use the **no** form of this command.

antenna count *0 - 8*

Syntax Description

0-8	Specifies the antenna count.

Command Default

None

Command Modes

Wireless radio profile configuration mode

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.6.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows you how to configure the number of antennas to be enabled under a radio profile:

```
Device# configure terminal
Device(config)# wireless profile radio radio-profile-name
Device(config-wireless-radio-profile)# antenna count 4
```

antenna monitoring

To configure antenna disconnection detection, use the **antenna monitoring** command. To disable antenna disconnection detection, use the **no** form of this command.

antenna monitoring [**rssi-failure-threshold** *threshold-value* | **weak-rssi** *weak-rssi-value* | **detection-time** *detect-time-in-mins*]

no antenna monitoring

Syntax Description

rssi-failure-threshold *threshold-value*	Configures RSSI failure threshold value, in dB. Valid values range from 10 to 90, with a default of 40. The *threshold-value* determines the signal strength delta across the received antennas of the AP.
weak-rssi *weak-rssi-value*	Configures weak RSSI value, in dBm. Valid values range from -90 to -10, with a default of 60. If the RSSI received by the AP is greater or equal to the configured *weak-rssi-value*, the antenna is considered as broken. Configuration of the *weak-rssi-value* is based on the deployment of the neighbor AP distance.
detection-time *detect-time-in-mins*	Configures the antenna disconnection detection time, in minutes. Valid values range from 9 to 180, with a default of 120. The *detect-time-in-mins* is used to monitor the signal strength (both *weak-rssi-value* and *threshold-value* criteria) before flagging it as a problem.

Command Default

Antenna monitoring is not enabled.

Command Modes

AP profile configuration (config-ap-profile)

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.4.1	This command was introduced.

Usage Guidelines

This command is supported only on the following APs:

- Cisco Catalyst 9120AX Series Access Points
- Cisco Catalyst 9130AX Series Access Points
- Cisco Aironet 2800e Access Points
- Cisco Aironet 3800e Access Points

Example

The following example shows how to enable antenna disconnection detection:

```
Device# configure terminal
Device(config)# ap profile xyz-ap-profile
Device(config-ap-profile)# antenna monitoring
```

ap

To configure cisco APs, use the **ap** command.

ap *mac-address*

Syntax Description

mac-address	Ethernet MAC address of the AP.

Command Default

None

Command Modes

config

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines

none.

Example

The following example shows how to configure a Cisco AP:

```
Device(config)# ap F866.F267.7DFB
```

ap audit-report

To enable or configure AP audit reporting, use the **ap audit-report** command.

ap audit-report {**enable** | **interval** *interval*}

Syntax Description

enable	Enables AP audit reporting.
interval	Configures the AP audit report interval.
interval	AP audit report interval, in minutes. Default is 1440. The valid range is from 0 to 43200.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.3.1	This command was introduced.

Example

The following example shows how to configure AP audit report interval:

```
Device(config)# ap audit-report interval 1300
```

ap auth-list

To configure the AP authorization list, use the **ap auth-list** command in the global configuration mode. To disable the AP authorization list, use the **no** form of this command.

ap auth-list {**authorize-mac** | **authorize-serialNum** | **method-list** *method-list-name*}

no ap auth-list {**authorize-mac** | **authorize-serialNum** | **method-list** *method-list-name*}

Syntax Description

authorize-mac	Configures the AP authorization policy with MAC.
auhorize-serialNum	Configures the AP authorization policy with the serial number.
method-list	Configures the AP authorization method list.
method-list-name	Indicates the method list name.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Example

The following example shows how to configure the AP authorization policy with serial number:

```
Device(config) #ap auth-list authorize-serialNum
```

ap auth-list ap-cert-policy allow-mic-ap

To enable the AP certificate policy during CAPWAP-DTLS handshake, use the **ap auth-list ap-cert-policy allow-mic-ap** command, in the global configuration mode. To disable the AP certificate policy during CAPWAP-DTLS handshake, use the **no** form of this command.

ap auth-list ap-cert-policy allow-mic-ap

no ap auth-list ap-cert-policy allow-mic-ap

Syntax Description

This command has no arguments or keywords.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.5.1	This command was introduced.

Example

The following example shows how to configure AP certificate policy during CAPWAP-DTLS handshake:

```
Device# configure terminal
Device(config)# ap auth-list ap-cert-policy
Device(config)# ap auth-list ap-cert-policy allow-mic-ap
```

ap auth-list ap-cert-policy allow-mic-ap trustpoint

To configure the trustpoint name for the controller certificate chain, use the **ap auth-list ap-cert-policy allow-mic-ap trustpoint** command, in the global configuration mode. To disable the feature, use the **no** form of the command.

ap auth-list ap-cert-policy allow-mic-ap trustpoint

no ap auth-list ap-cert-policy allow-mic-ap trustpoint

Syntax Description

trustpoint-name	Specifies the trustpoint name for the wireless controller certificate chain.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.5.1	This command was introduced.

Example

The following example shows how to the trustpoint name for the controller certificate chain:

```
Device# configure terminal
Device(config)# ap auth-list ap-cert-policy
Device(config)# ap auth-list ap-cert-policy allow-mic-ap trustpoint trustpoint-name
```

ap auth-list ap-cert-policy mac-address MAC-address | serial-number AP-serial-number policy-type mic

To configure the AP certificate policy based on the Ethernet MAC address or based on the assembly serial number of the AP, use the **ap auth-list ap-cert-policy** {**mac-address** *H.H.H* | **serial-number** *AP-serial-number*} **policy-type mic** command. Use the **no** form of this command to disable the feature.

ap auth-list ap-cert-policy { **mac-address** *H.H.H* | **serial-number** *AP-serial-number* } **policy-type mic**

no ap auth-list ap-cert-policy { **mac-address** *H.H.H* | **serial-number** *AP-serial-number* } **policy-type mic**

Syntax Description

ap auth-list	Configure the authorization list of the Access Point.
ap-cert-policy	Specifies the AP Certificate Policy during CAPWAP DTLS.
mac-address *MAC-address*	Configures AP cert policy based on Ethernet MAC.
serial-number *AP-serial-number*	Configure AP cert policy based on Serial Number.
policy-type	Configures AP certificate policy type.
mic	Selects MIC AP policy.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.5.1	This command was introduced.

Example

The following example shows how to configure the AP certificate policy based on the Ethernet MAC address or based on the assembly serial number of the AP:

```
Device# configure terminal
Device(config)# ap auth-list ap-cert-policy mac-address 10.1.1 policy-type mic

Device(config)# ap auth-list ap-cert-policy serial-number ap-serial-number policy-type mic
```

ap auth-list ap-policy

To configure authorization policy for all Cisco lightweight access points joined to the device, use the **ap auth-list ap-policy** command. To disable authorization policy for all Cisco lightweight access points joined to the device, use the **no** form of this command.

ap auth-list ap-policy {**authorize-ap** | **lsc** | **mic** | **ssc**}
no ap auth-list ap-policy {**authorize-ap** | **lsc** | **mic** | **ssc**}

Syntax Description

authorize-ap	Enables the authorization policy.
lsc	Enables access points with locally significant certificates to connect.
mic	Enables access points with manufacture-installed certificates to connect.
ssc	Enables access points with self signed certificates to connect.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

This example shows how to enable the access point authorization policy:

```
Device(config)# ap auth-list ap-policy authorize-ap
```

This example shows how to enable access points with locally significant certificates to connect:

```
Device(config)# ap auth-list ap-policy lsc
```

This example shows how to enable access points with manufacture-installed certificates to connect:

```
Device(config)# ap auth-list ap-policy mic
```

This example shows how to enable access points with self-signed certificates to connect:

```
Device(config)# ap auth-list ap-policy ssc
```

ap auth-list method-list MY-METHOD-LIST mac

To set the AP authorization method list to be used for AP MAC authorization, use the **ap auth-list method-list** *My-Method-List***mac** command.

ap auth-list method-list *My-Method-List* **mac**

Syntax Description

My-Method-List	Specifies the AP authorization method list.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.18.1	This command was introduced.

Examples

The following example shows how toset the AP authorization method list to be used for AP MAC authorization:

```
Device# configure terminal
Device(config)# ap auth-list method-list MY-METHOD-LIST mac
Device(config-sg-radius)# exit
```

ap capwap multicast

To configure the multicast address used by all access points to receive multicast traffic when multicast forwarding is enabled and to configure the outer Quality of Service (QoS) level of those multicast packets sent to the access points, use the **ap capwap multicast** command.

ap capwap multicast {*multicast-ip-address* | **service-policy output** *pollicymap-name*}

Syntax Description

multicast-ip-address	Multicast IP address.
service-policy	Specifies the tunnel QoS policy for multicast access points.
output	Assigns a policy map name to the output.
policymap-name	Service policy map name.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

This example shows how to configure a multicast address used by all access points to receive multicast traffic when multicast forwarding is enabled:

```
Device(config)# ap capwap multicast 239.2.2.2
```

This example shows how to configure a tunnel multicast QoS service policy for multicast access points:

```
Device(config)# ap capwap multicast service-policy output tunnmulpolicy
```

ap capwap retransmit

To configure Control and Provisioning of Wireless Access Points (CAPWAP) control packet retransmit count and control packet retransmit interval under the AP profile, use the **ap capwap retransmit** command.

ap profile default-ap-profile

ap capwap retransmit {**count** *retransmit-count* | **interval** *retransmit-interval*}

Syntax Description

count *retransmit-count*	Specifies the access point CAPWAP control packet retransmit count. **Note** The count is from 3 to 8 seconds.
interval *retransmit-interval*	Specifies the access point CAPWAP control packet retransmit interval. **Note** The interval is from 2 to 5 seconds.

Command Default

None

Command Modes

AP profile configuration (config-ap-profile)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

This example shows how to configure the CAPWAP control packet retransmit count for an access point:

```
Device# ap capwap retransmit count 3
```

This example shows how to configure the CAPWAP control packet retransmit interval for an access point:

```
Device# ap capwap retransmit interval 5
```

ap capwap timers

To configure advanced timer settings under the AP profile mode, use the **ap capwap timers** command.

ap profile default-ap-profile

ap capwap timers {**discovery-timeout** *seconds* | **fast-heartbeat-timeout local** *seconds* | **heartbeat-timeout** *seconds* | **primary-discovery-timeout** *seconds* | **primed-join-timeout** *seconds*}

Syntax Description

discovery-timeout	Specifies the Cisco lightweight access point discovery timeout. **Note** The Cisco lightweight access point discovery timeout is how long a Cisco device waits for an unresponsive access point to answer before considering that the access point failed to respond.
seconds	Cisco lightweight access point discovery timeout from 1 to 10 seconds. **Note** The default is 10 seconds.
fast-heartbeat-timeout local	Enables the fast heartbeat timer that reduces the amount of time it takes to detect a device failure for local or all access points.
seconds	Small heartbeat interval (from 1 to 10 seconds) that reduces the amount of time it takes to detect a device failure. **Note** The fast heartbeat time-out interval is disabled by default.
heartbeat-timeout	Specifies the Cisco lightweight access point heartbeat timeout. **Note** The Cisco lightweight access point heartbeat timeout controls how often the Cisco lightweight access point sends a heartbeat keep-alive signal to the Cisco device. This value should be at least three times larger than the fast heartbeat timer.
seconds	Cisco lightweight access point heartbeat timeout value from 1 to 30 seconds. **Note** The default is 30 seconds.
primary-discovery-timeout	Specifies the access point primary discovery request timer. The timer determines the amount of time taken by an access point to discovery the configured primary, secondary, or tertiary device.
seconds	Access point primary discovery request timer from 30 to 3600 seconds. **Note** The default is 120 seconds.

primed-join-timeout	Specifies the authentication timeout. Determines the time taken by an access point to determine that the primary device has become unresponsive. The access point makes no further attempts to join the device until the connection to the device is restored.
seconds	Authentication response timeout from 120 to 43200 seconds. **Note** The default is 120 seconds.

Command Default

None

Command Modes

AP profile mode (config-ap-profile)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

This example shows how to configure an access point discovery timeout with the timeout value of 7:

```
Device(config)# ap profile default-ap-profile

Device(config-ap-profile)# ap capwap timers discovery-timeout 7
```

This example shows how to enable the fast heartbeat interval for all access points:

```
Device(config)# ap profile default-ap-profile

Device(config-ap-profile)# ap capwap timers fast-heartbeat-timeout 6
```

This example shows how to configure an access point heartbeat timeout to 20:

```
Device(config)# ap profile default-ap-profile

Device(config-ap-profile)# ap capwap timers heartbeat-timeout 20
```

This example shows how to configure the access point primary discovery request timer to 1200 seconds:

```
Device(config)# ap profile default-ap-profile

Device(config-ap-profile)# ap capwap timers primary-discovery-timeout 1200
```

This example shows how to configure the authentication timeout to 360 seconds:

```
Device(config)# ap profile default-ap-profile

Device(config-ap-profile)# ap capwap timers primed-join-timeout 360
```

ap cisco-dna token

To configure Cisco DNA token, use the **ap cisco-dna token** command. To disable the configuration, use the no form of the command.

ap cisco-dna token { **0** | **8** } <*cisco-token-number*>

no ap cisco-dna token

Syntax Description

Cisco-dna	Configures Cisco DNA parameters.
token	Configures Cisco DNA token.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.3.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows how to configure Cisco DNA token:

```
Device(config)# ap cisco-dna token 0 <cisco-token-number>
```

ap country

To configure one or more country codes for a device, use the **ap country** command.

ap country *country-code*

Syntax Description

country-code	Two-letter or three-letter country code or several country codes separated by a comma.

Command Default

US (country code of the United States of America).

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
Cisco IOS XE Amsterdam 17.3.1	This command has been deprecated. **Note** From Cisco IOS XE Amsterdam 17.3.1 onwards, the command **ap country** is deprecated and renamed as **wireless country** *<1 country code>*, where you can enter country codes for more than 20 countries. Although the existing command **ap country** is still functional, it is recommended that you use the **wireless country** *<1 country code>* command.

Usage Guidelines

The Cisco device must be installed by a network administrator or qualified IT professional and the installer must select the proper country code. Following installation, access to the unit should be password protected by the installer to maintain compliance with regulatory requirements and to ensure proper unit functionality. See the related product guide for the most recent country codes and regulatory domains.

This example shows how to configure country codes on the device to IN (India) and FR (France):

```
Device(config)# ap country IN,FR
```

ap dot11 5ghz rrm channel unii3-low-power-channels

To configure UNII-3-low power channels for 5-GHz band, use the **ap dot11 5ghz rrm channel unii3-low-power-channels** command.

ap dot11 5ghz rrm channel unii3-low-power-channels

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Dublin 17.17.1	This command was introduced.

Examples

The following example shows how to configure UNII-3-low power channels for 5-GHz band:

```
Device(config)# ap dot11 5ghz rrm channel unii3-low-power-channels
```

ap dot11 24ghz | 5ghz dot11ax spatial-reuse obss-pd

To configure the 802.11ax OBSS PD based spatial reuse on all 2.4-GHz or 5-GHz radios, use the **ap dot11** {**24ghz** | **5ghz**} **dot11ax spatial-reuse obss-pd** command. To disable the OBSS based spatial reuse feature, use the **no** form of this command.

ap dot11 { **24ghz** | **5ghz** } **dot11ax spatial-reuse obss-pd**

no ap dot11 { **24ghz** | **5ghz** } **dot11ax spatial-reuse obss-pd**

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.4.1	This command was introduced.

Example

The following example shows how to configure the 802.11ax OBSS PD based spatial reuse:

```
Device(config)# ap dot11 24ghz or 5ghz dot11ax spatial-reuse obss-pd
```

ap dot11 24ghz | 5ghz dot11ax spatial-reuse obss-pd non-srg-max

To configure 802.11ax non-Spatial Reuse Groups (SRG) OBSS PD max on all 2.4-GHz or 5-GHz radios, use the **ap dot11** { **24ghz** | **5ghz** } **dot11ax spatial-reuse obss-pd non-srg-max** *-82 - -62* command. To disable the 802.11ax non-Spatial Reuse Groups (SRG) OBSS PD max on all 2.4-GHz or 5-GHz radios, use the **no** form of this command.

ap dot11 { **24ghz** | **5ghz** } **dot11ax spatial-reuse obss-pd non-srg-max** *-82 - -62*

no ap dot11 { **24ghz** | **5ghz** } **dot11ax spatial-reuse obss-pd non-srg-max** *-82 - -62*

Syntax Description

-82 - -62	Specifies the non-SRG OBSS PD max value in dBm

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.4.1	This command was introduced.

Example

The following example shows how to configure 802.11ax non-SRG OBSS PD max on all 2.4-GHz or 5-GHz radios.:

```
Device(config)# ap dot11 24ghz or 5ghz dot11ax spatial-reuse obss-pd non-srg-max -80
```

ap dot11 24ghz | 5ghz rrm ndp-mode

To configure the operating mode for 802.11a neighbor discovery, use the **ap dot11** {**24ghz** | **5ghz**} **rrm ndp-mode** command.

ap dot11 { **24ghz** | **5ghz** } **rrm ndp-mode** { **auto** | **off-channel** }

Syntax Description

auto	Enables the auto mode.
off-channel	Enables NDP packets on RF ASIC radio.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.5.1	This command was introduced.

Example

The following example shows how to configure the operating mode for 802.11a neighbor discovery:

```
Device# configure terminal
Device(config)# ap dot11 24ghz or 5ghz rrm ndp-mode auto
```

ap dot11 24ghz cleanair

To enable CleanAir for detecting 2.4-GHz devices, use the **ap dot11 24ghz cleanair** command in global configuration mode. To disable CleanAir for detecting 2.4-GHz devices, use the **no** form of this command.

ap dot11 24ghz cleanair

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Global configuration (config).

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

You must enable this CleanAir command before you configure other CleanAir commands.

This example shows how to enable CleanAir for 2.4-GHz devices:

```
Device(config)# ap dot11 24ghz cleanair
```

default ap dot11 24ghz cleanair device

To configure the default state of report generation for 2.4-GHz interference devices, use the **default ap dot11 24ghz cleanair device** command in global configuration mode.

default ap dot11 24ghz cleanair device {**ble-beacon** | **bt-discovery** | **bt-link** | **canopy** | **cont-tx** | **dect-like** | **fh** | **inv** | **jammer** | **mw-oven** | **nonstd** | **report** | **superag** | **tdd-tx** | **video** | **wimax-fixed** | **wimax-mobile** | **xbox** | **zigbee**}

Syntax Description

ble-beacon	Configure the BLE beacon feature.
bt-discovery	Configures the alarm for Bluetooth interference devices.
bt-link	Configures the alarm for any Bluetooth link.
canopy	Configures the alarm for canopy interference devices.
cont-tx	Configures the alarm for continuous transmitters.
dect-like	Configures the alarm for Digital Enhanced Cordless Communication (DECT)-like phones.
fh	Configures the alarm for 802.11 frequency hopping devices.
inv	Configures the alarm for devices using spectrally inverted Wi-Fi signals.
jammer	Configures the alarm for jammer interference devices.
mw-oven	Configures the alarm for microwave ovens.
nonstd	Configures the alarm for devices using nonstandard Wi-Fi channels.
superag	Configures the alarm for 802.11 SuperAG interference devices.
tdd-tx	Configures the alarm for Time Division Duplex (TDD) transmitters.
video	Configures the alarm for video cameras.

wimax-fixed	Configures the alarm for WiMax fixed interference devices.
wimax-mobile	Configures the alarm for WiMax mobile interference devices.
xbox	Configures the alarm for Xbox interference devices.
zigbee	Configures the alarm for 802.15.4 interference devices.

Command Default

The alarm for Wi-Fi inverted devices is enabled. The alarm for all other devices is disabled.

Command Modes

Global configuration (config).

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
	This command was modified. The **ble-beacon** keyword was added.

Usage Guidelines

You must enable CleanAir using the **ap dot11 24ghz cleanair**command before you configure this command.

This example shows how to enable CleanAir to report when a video camera interferes:

```
Device(config)# default ap dot11 24ghz cleanair device video
```

ap dot11 24ghz dot11g

To enable the Cisco wireless LAN solution 802.11g network, use the **ap dot11 24ghz dot11g** command. To disable the Cisco wireless LAN solution 802.11g network, use the **no** form of this command.

ap dot11 24ghz dot11g
no ap dot11 24ghz dot11g

Syntax Description

This command has no keywords and arguments.

Command Default

Enabled

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

Before you enter the **ap dot11 24ghz dot11g** command, disable the 802.11 Cisco radio with the **ap dot11 24ghz shutdown** command.

After you configure the support for the 802.11g network, use the **no ap dot11 24ghz shutdown** command to enable the 802.11 2.4 Ghz radio.

This example shows how to enable the 802.11g network:

```
Device(config)# ap dot11 24ghz dot11g
```

ap dot11 24ghz rate

To configure 802.11b operational rates, use the **ap dot11 24ghz rate** command.

ap dot11 24ghz rate {**RATE_11M** | **RATE_12M** | **RATE_18M** | **RATE_1M** | **RATE_24M** | **RATE_2M** | **RATE_36M** | **RATE_48M** | **RATE_54M** | **RATE_5_5M** | **RATE_6M** | **RATE_9M**} {**disable** | **mandatory** | **supported**}

Syntax Description

RATE_11M	Configures the data to be transmitted at the rate of 11 Mbps
RATE_12M	Configures the data to be transmitted at the rate of 12 Mbps
RATE_18M	Configures the data to be transmitted at the rate of 18 Mbps
RATE_1M	Configures the data to be transmitted at the rate of 1 Mbps
RATE_24M	Configures the data to be transmitted at the rate of 24 Mbps
RATE_2M	Configures the data to be transmitted at the rate of 2 Mbps
RATE_36M	Configures the data to be transmitted at the rate of 36 Mbps
RATE_48M	Configures the data to be transmitted at the rate of 48 Mbps
RATE_54M	Configures the data to be transmitted at the rate of 54 Mbps
RATE_5_5M	Configures the data to be transmitted at the rate of 5.5 Mbps
RATE_6M	Configures the data to be transmitted at the rate of 6 Mbps
RATE_9M	Configures the data to be transmitted at the rate of 9 Mbps
disable	Disables the data rate that you specify. Also defines that the clients specify the data rates used for communication.
mandatory	Defines that the clients support this data rate in order to associate with an AP.
supported	Any associated clients support this data rate can communicate with the AP using this rate. However, the clients are not required to use this rate to associate with the AP.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure 802.11b operational rate to 9 Mbps and make it mandatory:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap dot11 24ghz rate RATE_9M mandatory
```

ap dot11 24ghz rf-profile default rf-profile

To configure an RF profile for WiFi-IoT coexistence, use the **ap dot11 24ghz rf-profile default rf-profile** command in the global configuration mode. Use the **no** form of this command to disable the feature.

ap dot11 24ghz rf-profile default rf-profile

no ap dot11 24ghz rf-profile default rf-profile

Syntax Description

This command has no keywords or arguments.

Command Default

The default is RF_PROFILE_NAME

Command Modes

Global configuration mode

Usage Guidelines

This is a default profile applied to all the APs. Users can modify it for coexistence enablement. The command default can be either default or custom.

Command History

Release	Modification
Cisco IOS XE 26.1.1	This command is introduced.

Examples

This example shows how to configure and enable ap dot11 24ghz rf-profile default rf-profile in the global configuration mode:

```
Device# configure terminal
Device(config)# ap dot11
Device(config)# ap dot11 24ghz
Device(config)# ap dot11 24ghz rf-profile
Device(config)# ap dot11 24ghz rf-profile default-rf-profile
Device(config)# exit
```

ap dot11 24ghz rrm channel cleanair-event

To enable Event-Driven RRM (EDRRM) and the sensitivity for 2.4-GHz devices, use the **ap dot11 24ghz rrm channel cleanair-event** command in global configuration mode. To disable EDRRM, use the **no** form of this command.

ap dot11 24ghz rrm channel cleanair-event sensitivity {**high** | **low** | **medium**}
no ap dot11 24ghz rrm channel cleanair-event [**sensitivity**{**high** | **low** | **medium**}]

Syntax Description

sensitivity	(Optional) Configures the EDRRM sensitivity of the CleanAir event.
high	(Optional) Specifies the highest sensitivity to non-Wi–Fi interference as indicated by the air quality (AQ) value.
low	(Optional) Specifies the least sensitivity to non-Wi–Fi interference as indicated by the AQ value.
medium	(Optional) Specifies medium sensitivity to non-Wi–Fi interference as indicated by the AQ value.

Command Default

EDRRM is disabled and the sensitivity is low.

Command Modes

Global configuration (config).

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

You must enable EDRRM using the **ap dot11 24ghz rrm channel cleanair-event** command before you configure the sensitivity.

This example shows how to enable EDRRM and set the EDRRM sensitivity to low:

```
Device(config)# ap dot11 24ghz rrm channel cleanair-event
Device(config)# ap dot11 24ghz rrm channel cleanair-event sensitivity low
```

ap dot11 24ghz rrm channel device

To configure persistent non-Wi-Fi device avoidance in the 802.11b channel, use the **ap dot11 24ghz rrm channel device** command in global configuration mode. To disable persistent device avoidance, use the **no** form of this command.

ap dot11 24ghz rrm channel device
no ap dot11 24ghz rrm channel device

Syntax Description

This command has no arguments or keywords.

Command Default

Persistent device avoidance is disabled.

Command Modes

Global configuration (config).

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

CleanAir-capable monitor mode access points collect information about persistent devices on all configured channels and stores the information in the device. Local and bridge mode access points detect interference devices on the serving channels only.

This example shows how to enable persistent device avoidance:

```
Device(config)# ap dot11 24ghz rrm channel device
```

ap dot11 24ghz rrm optimized-roam

To configure optimized roaming for 802.11b network, use the **ap dot11 24ghz rrm optimized-roam** command.

ap dot11 24ghz rrm optimized-roam [**data-rate-threshold** {**11M** | **12M** | **18M** | **1M** | **24M** | **2M** | **36M** | **48M** | **54M** | **5_5M** | **6M** | **9M** | **disable**}]

Syntax Description

data-rate-threshold	Configures the data rate threshold for 802.11b optimized roaming.
11M	Sets the data rate threshold for 802.11b optimized roaming to 11 Mbps
12M	Sets the data rate threshold for 802.11b optimized roaming to of 12 Mbps
18M	Sets the data rate threshold for 802.11b optimized roaming to of 18 Mbps
1M	Sets the data rate threshold for 802.11b optimized roaming to of 1 Mbps
24M	Sets the data rate threshold for 802.11b optimized roaming to of 24 Mbps
2M	Sets the data rate threshold for 802.11b optimized roaming to of 2 Mbps
36M	Sets the data rate threshold for 802.11b optimized roaming to of 36 Mbps
48M	Sets the data rate threshold for 802.11b optimized roaming to of 48 Mbps
54M	Sets the data rate threshold for 802.11b optimized roaming to of 54 Mbps
5_5M	Sets the data rate threshold for 802.11b optimized roaming to of 5.5 Mbps
6M	Sets the data rate threshold for 802.11b optimized roaming to of 6 Mbps
9M	Sets the data rate threshold for 802.11b optimized roaming to of 9 Mbps
disable	Disables the data rate threshold.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure optimized roaming for 802.11b network:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap dot11 24ghz rrm optimized-roam
```

ap dot11 24ghz rx-sop threshold

To configure 802.11b radio receiver start-of-packet (RxSOP), use the **ap dot11 24ghz rx-sop threshold** command.

ap dot11 24ghz rx-sop threshold {**auto** | **high** | **low** | **medium** | **custom** *rxsop-value*}

Syntax Description

auto	Reverts RxSOP value to the default value.
high	Sets the RxSOP value to high threshold (–79 dBm).
medium	Sets the RxSOP value to medium threshold (–82 dBm).
low	Sets the RxSOP value to low threshold (–85 dBm).
custom *rxsop-value*	Sets the RxSOP value to custom threshold (–85 dBm to –60 dBm)

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Usage Guidelines

RxSOP determines the Wi-Fi signal level in dBm at which an access point's radio demodulates and decodes a packet. Higher the level, less sensitive the radio is and smaller the receiver cell size. The table below shows the RxSOP threshold values for high, medium, low, and custom levels for 2.4-GHz band.

Table 2: RxSOP Thresholds for 2.4-GHz Band

High Threshold	Medium Threshold	Low Threshold	Custom Threshold
–79 dBm	–82 dBm	–85 dBm	–85 dBm to –60 dBm

Examples

The following example shows how to configure 802.11b radio receiver start-of-packet (RxSOP) value to auto:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap dot11 24ghz rx-sop threshold auto
```

ap dot11 24ghz shutdown

To disable 802.11a network, use the **ap dot11 24ghz shutdown** command.

ap dot11 24ghz shutdown

Command Default None

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to disable the 802.11a network:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap dot11 24ghz shutdown
```

ap dot11 5ghz channelswitch quiet

To configure the 802.11h channel switch quiet mode, use the **ap dot11 5ghz channelswitch quiet** command.

ap dot11 5ghz channelswitch quiet

Command Default None

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure the 802.11h channel switch quiet mode:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap dot11 5ghz channelswitch quiet
```

ap dot11 5ghz cleanair

To enable CleanAir for detecting 5-GHz devices, use the **ap dot11 5ghz cleanair** command in global configuration mode.

ap dot11 5ghz cleanair

Command Default

Disabled.

Command Modes

Global configuration.

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

You must enable this CleanAir command before you configure other CleanAir commands.

This example shows how to enable CleanAir for 5-GHz devices:

```
Device(config)# ap dot11 5ghz cleanair
```

default ap dot11 5ghz cleanair device

To configure the default state of the alarm for 5-GHz interference devices, use the **default ap dot11 5ghz cleanair device** command in global configuration mode.

default ap dot11 5ghz cleanair device {**canopy** | **cont-tx** | **dect-like** | **inv** | **jammer** | **nonstd** | **radar** | **report** | **superag** | **tdd-tx** | **video** | **wimax-fixed** | **wimax-mobile**}

Syntax Description

canopy	Configures the alarm for canopy interference devices.
cont-tx	Configures the alarm for continuous transmitters.
dect-like	Configures the alarm for Digital Enhanced Cordless Communication (DECT)-like phones.
inv	Configures the alarm for devices using spectrally inverted Wi-Fi signals.
jammer	Configures the alarm for jammer interference devices.
nonstd	Configures the alarm for devices using nonstandard Wi-Fi channels.
radar	Configures the alarm for radars.
report	Enables interference device reports.
superag	Configures the alarm for 802.11 SuperAG interference devices.
tdd-tx	Configures the alarm for Time Division Duplex (TDD) transmitters.
video	Configures the alarm for video cameras.
wimax-fixed	Configures the alarm for WiMax fixed interference devices.
wimax-mobile	Configures the alarm for WiMax mobile interference devices.

Command Default

The alarm for Wi-Fi inverted devices is enabled. The alarm for all other interference devices is disabled.

Command Modes

Global configuration (config).

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

You must enable CleanAir using the **ap dot11 5ghz cleanair** command before you configure this command.

This example shows how to enable CleanAir to report when a video camera interferes:

```
Device(config)# default ap dot11 5ghz cleanair device video
```

ap dot11 5ghz power-constraint

To configure the 802.11h power constraint value, use the **ap dot11 5ghz power-constraint** command. To remove the 802.11h power constraint value, use the **no** form of this command.

ap dot11 5ghz power-constraint *value*
no ap dot11 5ghz power-constraint

Syntax Description

value	802.11h power constraint value. **Note** The range is from 0 to 30 dBm.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

This example shows how to configure the 802.11h power constraint to 5 dBm:

```
Device(config)# ap dot11 5ghz power-constraint 5
```

ap dot11 5ghz rate

To configure 802.11a operational rates, use the **ap dot11 5ghz rate** command.

ap dot11 5ghz rate {**RATE_12M** | **RATE_18M** | **RATE_24M** | **RATE_36M** | **RATE_48M** | **RATE_54M** | **RATE_6M** | **RATE_9M**} {**disable** | **mandatory** | **supported**}

Syntax Description

RATE_12M	Configures the data to be transmitted at the rate of 12 Mbps
RATE_18M	Configures the data to be transmitted at the rate of 18 Mbps
RATE_24M	Configures the data to be transmitted at the rate of 24 Mbps
RATE_36M	Configures the data to be transmitted at the rate of 36 Mbps
RATE_48M	Configures the data to be transmitted at the rate of 48 Mbps
RATE_54M	Configures the data to be transmitted at the rate of 54 Mbps
RATE_6M	Configures the data to be transmitted at the rate of 6 Mbps
RATE_9M	Configures the data to be transmitted at the rate of 9 Mbps
disable	Disables the data rate that you specify. Also defines that the clients specify the data rates used for communication.
mandatory	Defines that the clients support this data rate in order to associate with an AP.
supported	Any associated clients support this data rate can communicate with the AP using this rate. However, the clients are not required to use this rate to associate with the AP.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure 802.11a operational rate to 24 Mbps and make it supported:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap dot11 5ghz rate RATE_24M supported
```

ap dot11 5ghz rrm channel cleanair-event

To enable Event-Driven RRM (EDRRM) and configure the sensitivity for 5-GHz devices, use the **ap dot11 5ghz rrm channel cleanair-event** command in global configuration mode. To disable EDRRM, use the **no** form of the command.

ap dot11 5ghz rrm channel cleanair-event [**sensitivity** {**high** | **low** | **medium**}]
no ap dot11 5ghz rrm channel cleanair-event [**sensitivity** {**high** | **low** | **medium**}]

Syntax Description

sensitivity	(Optional) Configures the EDRRM sensitivity of the CleanAir event.
high	(Optional) Specifies the highest sensitivity to non-Wi–Fi interference as indicated by the air quality (AQ) value.
low	(Optional) Specifies the least sensitivity to non-Wi–Fi interference as indicated by the AQ value.
medium	(Optional) Specifies medium sensitivity to non-Wi–Fi interference as indicated by the AQ value.

Command Default

EDRRM is disabled and the EDRRM sensitivity is low.

Command Modes

Global configuration (config).

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

You must enable EDRRM using the **ap dot11 5ghz rrm channel cleanair-event** command before you configure the sensitivity.

This example shows how to enable EDRRM and set the EDRRM sensitivity to high:

```
Device(config)# ap dot11 5ghz rrm channel cleanair-event
Device(config)# ap dot11 5ghz rrm channel cleanair-event sensitivity high
```

ap dot11 5ghz rrm channel device

To configure persistent non-Wi-Fi device avoidance in the 802.11a channel, use the **ap dot11 5ghz rrm channel device** command in global configuration mode. To disable persistent device avoidance, use the **no** form of this command.

ap dot11 5ghz rrm channel device
no ap dot11 5ghz rrm channel device

Syntax Description

This command has no arguments or keywords.

Command Default

The CleanAir persistent device state is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

CleanAir-capable monitor mode access points collect information about persistent devices on all configured channels and stores the information in the device. Local and bridge mode access points detect interference devices on the serving channels only.

This example shows how to enable persistent device avoidance on 802.11a devices:

```
Device(config)# ap dot11 5ghz rrm channel device
```

ap dot11 5ghz rrm channel zero-wait-dfs

To enable thes Zero Wait Dynamic Frequency Selection feature globally on 5-GHz devices, use the **ap dot11 5ghz rrm channel zero-wait-dfs** command. To disable the feature, use the **no** form of this command.

ap dot11 5ghz rrm channel zero-wait-dfs

no ap dot11 5ghz rrm channel zero-wait-dfs

Syntax Description

This command has no arguments or keywords.

Command Default

The Zero Wait Dynamic Frequency Selection feature is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Cupertino 17.9.1	This command was introduced.

Usage Guidelines

This command is applicable only on 5-GHz devices.

Examples

The following example shows how to enable the Zero Wait Dynamic Frequency Selection feature on 5-GHz devices:

```
Device# configure terminal
Device(config)# ap dot11 5ghz rrm channel zero-wait-dfs
```

ap dot11 5ghz rx-sop threshold

To configure 802.11a radio receiver start-of-packet (RxSOP), use the **ap dot11 5ghz rx-sop threshold** command.

ap dot11 5ghz rx-sop threshold {**auto** | **high** | **low** | **medium** | **custom** *rxsop-value*}

Syntax Description

auto	Reverts RxSOP value to the default value.
high	Sets the RxSOP value to high threshold (–76 dBm).
medium	Sets the RxSOP value to medium threshold (–78 dBm).
low	Sets the RxSOP value to low threshold (–80 dBm).
custom *rxsop-value*	Sets the RxSOP value to custom threshold (–85 dBm to –60 dBm)

Command Default

None

Command Modes

config

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Usage Guidelines

RxSOP determines the Wi-Fi signal level in dBm at which an access point's radio demodulates and decodes a packet. Higher the level, less sensitive the radio is and smaller the receiver cell size. The table below shows the RxSOP threshold values for high, medium, low, and custom levels for 5-GHz band.

Table 3: RxSOP Thresholds for 5-GHz Band

High Threshold	Medium Threshold	Low Threshold	Custom Threshold
–76 dBm	–78 dBm	–80 dBm	–85 dBm to –60 dBm

Examples

The following example shows how to configure 802.11b radio receiver start-of-packet (RxSOP) value to a custom value of –70 dBm:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap dot11 24ghz rx-sop threshold custom -70
```

ap dot11 5ghz shutdown

To disable 802.11a network, use the **ap dot11 5ghz shutdown** command.

ap dot11 5ghz shutdown

Command Default None

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to disable the 802.11a network:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap dot11 5ghz shutdown
```

ap dot11 5ghz smart-dfs

To configure to use nonoccupancy time for radar interference channel, use the **ap dot11 5ghz smart-dfs** command.

ap dot11 5ghz smart-dfs

Command Default None

Command Modes config

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure to use nonoccupancy time for radar interference channel:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap dot11 5ghz smart-dfs
```

ap dot11 6ghz cleanair

To configure the CleanAir features for the 6-GHz radios, use the **ap dot11 6ghz cleanair** command. Use the **no** form of this command to disable the feature.

ap dot11 6ghz cleanair

no ap dot11 6ghz cleanair

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global Configuration

Command History

Release	Modification
Cisco IOS XE Cupertino 17.9.1	The command was introduced.

Example

This example shows how to configure the CleanAir features for the 6-GHz radios:

```
Device# ap dot11 6ghz cleanair
```

ap dot11 6ghz rf-profile

To configure the RF profile for 802.11 6-GHz parameters, use the **ap dot11 6ghz rf-profile**

ap dot11 6ghz rf-profile *rf-profile-name*

Syntax Description

rf-profile-name	Specifies the RF profile name.

Command Default

None

Command Modes

Global Configuration

Command History

Release	Modification
Cisco IOS XE Cupertino 17.9.1	This command was introduced.

Example

This example shows how to configure the RF profile for 802.11 6-GHz parameters:

```
Device(config)# ap dot11 6ghz rf-profile rf-profile-name
```

ap dot11

To configure Spectrum Intelligence (SI) on Qualcomm based 2.4 GHz or 5 GHz radios, use the **ap dot11 SI** command.

ap dot11 {**24ghz** | **5ghz** } **SI**

Syntax Description

24ghz	2.4 GHz radio
5ghz	5 GHz radio
SI	Enable Spectrum Intelligence (SI). [no] in the command disasbles SI.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to enable SI on 5GHz radio:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap dot11 5ghz SI
```

ap dot11 beaconperiod

To change the beacon period globally for 2.4 GHz or 5 GHz bands, use the **ap dot11 beaconperiod** command.

Note Disable the 802.11 network before using this command. See the "Usage Guidelines" section.

ap dot11 {**24ghz** | **5ghz**} **beaconperiod** *time*

Syntax Description

24ghz	Specifies the settings for 2.4 GHz band.
5ghz	Specifies the settings for 5 GHz band.
beaconperiod	Specifies the beacon for a network globally.
time	Beacon interval in time units (TU). One TU is 1024 microseconds. The range is from 20 to 1000.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

In Cisco wireless LAN 802.11 networks, all Cisco lightweight access point wireless LANs broadcast a beacon at regular intervals. This beacon notifies clients that the wireless service is available and allows the clients to synchronize with the lightweight access point.

Before you change the beacon period, make sure that you have disabled the 802.11 network by using the **ap dot11** {**24ghz | 5ghz**} **shutdown** command. After changing the beacon period, enable the 802.11 network by using the **no ap dot11** {**24ghz | 5ghz**} **shutdown** command.

This example shows how to configure the 5 GHZ band for a beacon period of 120 time units:

```
Device(config)# ap dot11 5ghz beaconperiod 120
```

ap dot11 cac media-stream

To configure media stream Call Admission Control (CAC) voice and video quality parameters for 2.4 GHz and 5 GHz bands, use the **ap dot11 cac media-stream** command.

ap dot11 {**24ghz** | **5ghz**} **cac media-stream multicast-direct** {**max-retry-percent** *retryPercent* | **min-client-rate** {**eighteen** | **eleven** | **fiftyFour** | **fivePointFive** | **fortyEight** | **nine** | **oneFifty** | **oneFortyFourPointFour** | **oneThirty** | **oneThirtyFive** | **seventyTwoPointTwo** | **six** | **sixtyFive** | **thirtySix** | **threeHundred** | **twelve** | **twentyFour** | **two** | **twoSeventy**}}

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
multicast-direct	Specifies CAC parameters for multicast-direct media streams.
max-retry-percent	Specifies the percentage of maximum retries that are allowed for multicast-direct media streams.
retryPercent	Percentage of maximum retries that are allowed for multicast-direct media streams. **Note** The range is from 0 to 100.
min-client-rate	Specifies the minimum transmission data rate to the client for multicast-direct media streams (rate at which the client must transmit in order to receive multicast-direct unicast streams). If the transmission rate is below this rate, either the video will not start or the client may be classified as a bad client. The bad client video can be demoted for better effort QoS or subject to denial.

min-client-rate	You can choose the following rates: • **eighteen** • **eleven** • **fiftyFour** • **fivePointFive** • **fortyEight** • **nine** • **one** • **oneFifty** • **oneFortyFourPointFour** • **oneThirty** • **oneThirtyFive** • **seventyTwoPointTwo** • **six** • **sixtyFive** • **thirtySix** • **threeHundred** • **twelve** • **twentyFour** • **two** • **twoSeventy**

Command Default

The default value for the maximum retry percent is 80. If it exceeds 80, either the video will not start or the client might be classified as a bad client. The bad client video will be demoted for better effort QoS or is subject to denial.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

CAC commands require that the WLAN you are planning to modify is configured for the Wi-Fi Multimedia (WMM) protocol.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **wlan** *wlan_name* **shutdown** command.

- Disable the radio network you want to configure by entering the **ap dot11** {**24ghz | 5ghz**} **shutdown** command.
- Save the new configuration.
- Enable voice or video CAC for the network you want to configure by entering the **ap dot11** {**24ghz | 5ghz**} **cac voice acm** or **ap dot11** {**24ghz | 5ghz**} **cac video acm** commands.

This example shows how to configure the maximum retry percent for multicast-direct media streams as 90 on a 802.11a network:

```
Device(config)# ap dot11 5ghz cac media-stream multicast max-retry-percent 90
```

ap dot11 cac multimedia

To configure multimedia Call Admission Control (CAC) voice and video quality parameters for 2.4 GHz and 5 GHz bands, use the **ap dot11 cac multimedia** command.

ap dot11 {**24ghz** | **5ghz**} **cac multimedia max-bandwidth** *bandwidth*

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
max-bandwidth	Specifies the percentage of maximum bandwidth allocated to Wi-Fi Multimedia (WMM) clients for voice and video applications on the 2.4 GHz or 5 GHz band.
bandwidth	Percentage of the maximum bandwidth allocated to WMM clients for voice and video applications on the 802.11a or 802.11b/g network. Once the client reaches the specified value, the access point rejects new multimedia flows this radio band. The range is from 5 to 85%.

Command Default

The default value is 75%.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

CAC commands require that the WLAN you are planning to modify is configured for the Wi-Fi Multimedia (WMM) protocol.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **wlan** *wlan_name* **shutdown** command.
- Disable the radio network you want to configure by entering the **ap dot11** {**24ghz | 5ghz**} **shutdown** command.
- Save the new configuration.
- Enable voice or video CAC for the network you want to configure by entering the **ap dot11** {**24ghz | 5ghz**} **cac voice acm** or **ap dot11** {**24ghz | 5ghz**} **cac video acm** commands.

This example shows how to configure the percentage of the maximum bandwidth allocated to WMM clients for voice and video applications on the 5 GHz band:

```
Device(config)# ap dot11 5ghz cac multimedia max-bandwidth 5
```

ap dot11 cac voice

To configure Call Admission Control (CAC) parameters for the voice category, use the **ap dot11 cac voice** command.

ap dot11 {**24ghz** | **5ghz**} **cac voice** {**acm** | **load-based** | **max-bandwidth** *value* | **roam-bandwidth** *value* | **sip** [**bandwidth** *bw*] **sample-interval** *value* | **stream-size** *x* **max-streams** *y* | **tspec-inactivity-timeout** {**enable** | **ignore**}}

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
acm	Enables bandwidth-based voice CAC for the 2.4 GHz or 5 GHz band. **Note** To disable bandwidth-based voice CAC for the 2.4 GHz or 5 GHz band, use the **no ap dot11** {**24ghz | 5ghz**} **cac voice acm** command.
load-based	Enable load-based CAC on voice access category. **Note** To disable load-based CAC on voice access category for the 2.4 GHz or 5 GHz band, use the **no ap dot11** {**24ghz | 5ghz**} **cac voice load-based** command.
max-bandwidth	Sets the percentage of the maximum bandwidth allocated to clients for voice applications on the 2.4 GHz or 5 GHz band.
value	Bandwidth percentage value from 5 to 85%.
roam-bandwidth	Sets the percentage of the CAC maximum allocated bandwidth reserved for roaming voice clients on the 2.4 GHz or 5 GHz band.
value	Bandwidth percentage value from 0 to 85%.
sip	Specifies the CAC codec name and sample interval as parameters and calculates the required bandwidth per call for the 802.11 networks.
bandwidth	(Optional) Specifies bandwidth for a SIP-based call.

bw	Bandwidth in kbps. The following bandwidth values specify parameters for the SIP codecs: • 64kbps—Specifies CAC parameters for the SIP G711 codec. • 8kbps—Specifies CAC parameters for the SIP G729 codec. **Note** The default value is 64 Kbps.
sample-interval	Specifies the packetization interval for SIP codec.
value	Packetization interval in msecs. The sample interval for SIP codec value is 20 seconds.
stream-size	Specifies the number of aggregated voice Wi-Fi Multimedia (WMM) traffic specification (TSPEC) streams at a specified data rate for the 2.4 GHz or 5 GHz band.
x	Stream size. The range of the stream size is from 84000 to 92100.
max-streams	Specifies the maximum number of streams per TSPEC.
y	Number (1 to 5) of voice streams. **Note** The default number of streams is 2 and the mean data rate of a stream is 84 kbps.
tspec-inactivity-timeout	Specifies TSPEC inactivity timeout processing mode. **Note** Use this keyword to process or ignore the Wi-Fi Multimedia (WMM) traffic specifications (TSPEC) inactivity timeout received from an access point. When the inactivity timeout is ignored, a client TSPEC is not deleted even if the access point reports an inactivity timeout for that client.
enable	Processes the TSPEC inactivity timeout messages.
ignore	Ignores the TSPEC inactivity timeout messages. **Note** The default is **ignore** (disabled).

Command Default None

Command Modes Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

CAC commands require that the WLAN you are planning to modify is configured for the Wi-Fi Multimedia (WMM) protocol and the quality of service (QoS) level be set to Platinum.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **wlan** *wlan_name* **shutdown** command.
- Disable the radio network you want to configure by entering the **ap dot11** {**24ghz | 5ghz**} **shutdown** command.
- Save the new configuration.
- Enable voice or video CAC for the network you want to configure by entering the **ap dot11** {**24ghz | 5ghz**} **cac voice acm** or **ap dot11** {**24ghz | 5ghz**} **cac video acm** commands.

This example shows how to enable the bandwidth-based CAC:

```
Device(config)# ap dot11 24ghz cac voice acm
```

This example shows how to enable the load-based CAC on the voice access category:

```
Device(config)# ap dot11 24ghz cac voice load-based
```

This example shows how to specify the percentage of the maximum allocated bandwidth for voice applications on the selected radio band:

```
Device(config)# ap dot11 24ghz cac voice max-bandwidth 50
```

This example shows how to configure the percentage of the maximum allocated bandwidth reserved for roaming voice clients on the selected radio band:

```
Device(config)# ap dot11 24ghz cac voice roam-bandwidth 10
```

This example shows how to configure the bandwidth and voice packetization interval for the G729 SIP codec on a 2.4 GHz band:

```
Device(config)# ap dot11 24ghz cac voice sip bandwidth 8 sample-interval 40
```

This example shows how to configure the number of aggregated voice traffic specifications stream with a stream size of 85000 and with a maximum of 5 streams:

```
Device(config)# ap dot11 24ghz cac voice stream-size 85000 max-streams 5
```

This example shows how to enable the voice TSPEC inactivity timeout messages received from an access point:

```
Device(config)# ap dot11 24ghz cac voice tspec-inactivity-timeout enable
```

ap dot11 cleanair

To configure CleanAir on 802.11 networks, use the **ap dot11 cleanair** command. To disable CleanAir on 802.11 networks, use the **no** form of this command.

ap dot11 {**24ghz** | **5ghz**} **cleanair**
no ap dot11 {**24ghz** | **5ghz**} **cleanair**

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
cleanair	Specifies CleanAir on the 2.4 GHz or 5 GHz band.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

This example shows how to enable the CleanAir settings on the 2.4 GHz band:

```
Device(config)# ap dot11 24ghz cleanair
```

ap dot11 cleanair alarm air-quality

To configure the CleanAir alarm for air quality in the 2.4-GHz or 5-GHz radios, use the **ap dot11** {**24ghz** | **5ghz**} **cleanair alarm air-quality**

ap dot11 { **24ghz** | **5ghz** } **cleanair alarm air-quality**

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global Configuration

Command History

Release	Modification
Cisco IOS XE Cupertino 17.9.1	This command was introduced.

Example

This example shows how to configure the CleanAir alarm for air quality in the 2.4-GHz or 5-GHz radios:

```
Device(config)# ap dot11 24ghz cleanair alarm air-quality
```

ap dot11 cleanair alarm air-quality threshold

To configure the air quality alarm threshold for the 2.4-GHz or 5-GHz radios, use the **ap dot11** {**24ghz** | **5ghz**} **cleanair alarm air-quality threshold**

ap dot11 { **24ghz** | **5ghz** } **cleanair alarm air-quality threshold** *threshold-value*

Syntax Description

threshold-value	Specifies the air quality alarm threshold value. The value range is from 1 to 100.

Command Default

None

Command Modes

Global Configuration

Command History

Release	Modification
Cisco IOS XE Cupertino 17.9.1	This command was introduced.

Example

This example shows how to configure the air quality alarm threshold for the 2.4-GHz or 5-GHz radios:

```
Device(config)# ap dot11 24ghz cleanair alarm air-quality threshold 25
```

ap dot11 cleanair alarm device cont-tx

To configure the continuous transmitter as the interference device CleanAir alarm in the 2.4-GHz or 5-GHz radios, use the **ap dot11** {**24ghz** | **5ghz**} **cleanair alarm device cont-tx**

ap dot11 { **24ghz** | **5ghz** } **cleanair alarm device cont-tx**

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global Configuration

Command History

Release	Modification
Cisco IOS XE Cupertino 17.9.1	This command was introduced.

Example

This example shows how to configure the continuous transmitter as the interference device CleanAir alarm in the 2.4-GHz or 5-GHz radios:

```
Device(config)# ap dot11 24ghz cleanair alarm device cont-tx
```

ap dot11 cleanair alarm unclassified

To configure air quality alarm on exceeding unclassified category severity in the 2.4-GHz and 5-GHz radios, use the **ap dot11** {**24ghz** | **5ghz**} **cleanair alarm unclassified**

ap dot11 { **24ghz** | **5ghz** } **cleanair alarm unclassified**

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global Configuration

Command History

Release	Modification
Cisco IOS XE Cupertino 17.9.1	This command was introduced.

Example

This example shows how to configure air quality alarm on exceeding unclassified category severity in the 2.4-GHz and 5-GHz radios:

```
Device(config)# ap dot11 24ghz cleanair alarm unclassified
```

ap dot11 cleanair alarm unclassified threshold

To configure air quality alarm on exceeding unclassified category severity in the 2.4-GHz and 5-GHz radios, use the **ap dot11** {**24ghz** | **5ghz**} **cleanair alarm unclassified threshold**

ap dot11 { **24ghz** | **5ghz** } **cleanair alarm unclassified threshold** *threshold-value*

Syntax Description

threshold-value	Specifies the air quality alarm on exceeding unclassified threshold value. The value range is from 1 to 100, where 1 is low interference and 100 is high interference.

Command Default

None

Command Modes

Global Configuration

Command History

Release	Modification
Cisco IOS XE Cupertino 17.9.1	This command was introduced.

Example

This example shows how to configure air quality alarm on exceeding unclassified category severity in the 2.4-GHz and 5-GHz radios:

```
Device(config)# ap dot11 24ghz cleanair alarm unclassified threshold 20
```

ap dot11 cleanair device

To configure CleanAir interference device types, use the **ap dot11 cleanair device** command.

ap dot11 24ghz cleanair device [**all** | **bt-discovery** | **bt-link** | **canopy** | **cont-tx** | **dect-like** | **fh** | **inv** | **jammer** | **mw-oven** | **nonstd** | **superag** | **tdd-tx** | **video** | **wimax-fixed** | **wimax-mobile** | **xbox** | **zigbee**]

Syntax Description

all	Specifies all device types.
device	Specifies the CleanAir interference device type.
bt-discovery	Specifies the Bluetooth device in discovery mode.
bt-link	Specifies the Bluetooth active link.
canopy	Specifies the Canopy devices.
cont-tx	Specifies the continuous transmitter.
dect-like	Specifies a Digital Enhanced Cordless Communication (DECT)-like phone.
fh	Specifies the 802.11 frequency hopping devices.
inv	Specifies the devices using spectrally inverted Wi-Fi signals.
jammer	Specifies the jammer.
mw-oven	Specifies the microwave oven devices.
nonstd	Specifies the devices using nonstandard Wi-Fi channels.
superag	Specifies 802.11 SuperAG devices.
tdd-tx	Specifies the TDD transmitter.
video	Specifies video cameras.
wimax-fixed	Specifies a WiMax fixed device.
wimax-mobile	Specifies a WiMax mobile device.
xbox	Configures the alarm for Xbox interference devices.
zigbee	Configures the alarm for 802.15.4 interference devices.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

This example shows how to configure the device to monitor ZigBee interferences:

```
Device(config)# ap dot11 24ghz cleanair device report
```

ap dot11 dot11be

To configure the 802.11be MCS rate index and spatial stream settings, use the **ap dot11 dot11be** command.

ap dot11 { **24ghz** | **5ghz** } **dot11be** [**mcs tx index** { **11** | **13** | **14** | **15** | **9** } **spatial-stream** *1-4*]

Syntax Description

mcs tx index	Specifies the modulation and coding scheme (MCS) rate index at which data can be transmitted between the access point and the client.
{**11** | **13** | **14** | **15** | **9**}	Specifies the 802.11be MCS rate indices.
spatial-stream	Configures the spatial-stream parameters.
1-4	Specifies the 802.11be spatial stream value.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Cisco IOS XE 17.15.1	This command was introduced.

Examples

The following example shows you how to configure the 802.11be MCS rate index and spatial stream settings:

```
Device# configure terminal
Device(config)# ap dot11 6ghz dot11be mcs tx index 11 spatial-stream 2
```

ap dot11 dot11n

To configure settings for an 802.11n network, use the **ap dot11 dot11n** command.

ap dot11 {**24ghz** | **5ghz**} **dot11n** {**a-mpdu tx priority** {*priority_value* **all** } | **scheduler timeout rt** *scheduler_value*} | **a-msdu tx priority** {*priority_value* | **all**} | **guard-interval** {**any** | **long**} | **mcs tx** *rate* | **rifs rx**}

Syntax Description

24ghz	Specifies the 2.4-GHz band.
5ghz	Specifies the 5-GHz band.
dot11n	Enables 802.11n support.
a-mpdu tx priority	Specifies the traffic that is associated with the priority level that uses Aggregated MAC Protocol Data Unit (A-MPDU) transmission.
priority_value	Aggregated MAC protocol data unit priority level from 0 to 7.
all	Specifies all of the priority levels at once.
a-msdu tx priority	Specifies the traffic that is associated with the priority level that uses Aggregated MAC Service Data Unit (A-MSDU) transmission.
priority_value	Aggregated MAC protocol data unit priority level from 0 to 7.
all	Specifies all of the priority levels at once.
scheduler timeout rt	Configures the 802.11n A-MPDU transmit aggregation scheduler timeout value in milliseconds.
scheduler_value	The 802.11n A-MPDU transmit aggregation scheduler timeout value from 1 to 10000 milliseconds.
guard-interval	Specifies the guard interval.
any	Enables either a short or a long guard interval.
long	Enables only a long guard interval.
mcs tx *rate*	Specifies the modulation and coding scheme (MCS) rates at which data can be transmitted between the access point and the client.
rate	Specifies the modulation and coding scheme data rates. **Note** The range is from 0 to 23.

rifs rx	Specifies the Reduced Interframe Space (RIFS) between data frames.

Command Default

By default, priority 0 is enabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

Aggregation is the process of grouping packet data frames together rather than transmitting them separately. The two aggregation methods available are:

- A-MPDU—This aggregation is performed in the software.
- A-MSDU—This aggregation is performed in the hardware

Aggregated MAC Protocol Data Unit priority levels assigned per traffic type are as follows:

- 0—Best effort
- 1—Background
- 2—Spare
- 3—Excellent effort
- 4—Controlled load
- 5—Video, less than 100-ms latency and jitter
- 6—Voice, less than 10-ms latency and jitter
- 7—Network control
- all—Configure all of the priority levels at once.



Note Configure the priority levels to match the aggregation method used by the clients.

This example shows how to enable 802.11n support on a 2.4-GHz band:

```
Device(config)# ap dot11 24ghz dot11n
```

This example shows how to configure all the priority levels at once so that the traffic that is associated with the priority level uses A-MSDU transmission:

```
Device(config)# ap dot11 24ghz dot11n a-msdu tx priority all
```

This example shows how to enable only long guard intervals:

```
Device(config)# ap dot11 24ghz dot11n guard-interval long
```

This example shows how to specify MCS rates:

```
Device(config)# ap dot11 24ghz dot11n mcs tx 5
```

This example shows how to enable RIFS:

```
Device(config)# ap dot11 24ghz dot11n rifs rx
```

ap dot11 dtpc

To configure Dynamic Transmit Power Control (DTPC) settings, Cisco Client eXtension (CCX) version 5 expedited bandwidth request feature, and the fragmentation threshold on an 802.11 network, use the **ap dot11 dtpc** command.

ap dot11 {**24ghz** | **5ghz**} {**dtpc** | **exp-bwreq** | **fragmentation** *threshold*}

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
dtpc	Specifies Dynamic Transport Power Control (DTPC) settings. **Note** This option is enabled by default.
exp-bwreq	Specifies Cisco Client eXtension (CCX) version 5 expedited bandwidth request feature. **Note** The expedited bandwidth request feature is disabled by default.
fragmentation *threshold*	Specifies the fragmentation threshold. **Note** This option can only used be when the network is disabled using the **ap dot11** {**24ghz	5ghz**} **shutdown** command.
threshold	Threshold. The range is from 256 to 2346 bytes (inclusive).

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

When the CCX version 5 expedited bandwidth request feature is enabled, the device configures all joining access points for this feature.

This example shows how to enable DTPC for the 5 GHz band:

```
Device(config)# ap dot11 5ghz dtpc
```

This example shows how to enable the CCX expedited bandwidth settings:

```
Device(config)# ap dot11 5ghz exp-bwrep
```

This example shows how to configure the fragmentation threshold on the 5 GHz band with the threshold number of 1500 bytes:

```
Device(config)# ap dot11 5ghz fragmentation 1500
```

ap dot11 edca-parameters

To enable a specific enhanced distributed channel access (EDCA) profile on the 2.4 GHz or 5 GHz bands, use the **ap dot11 edca-parameters** command. To disable an EDCA profile on the 2.4 GHz or 5 GHz bands, use the **no** form of this command.

ap dot11 { **24ghz** | **5ghz** } **edca-parameters** { **client-load-based** | **custom-voice** | **optimized-video-voice** | **optimized-voice** | **svp-voice** | **wmm-default** }
no ap dot11 { **24ghz** | **5ghz** } **edca-parameters** { **client-load-based** | **custom-voice** | **fastlane** | **optimized-video-voice** | **optimized-voice** | **svp-voice** | **wmm-default** }

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
edca-parameters	Specifies a specific enhanced distributed channel access (EDCA) profile on the 802.11 networks.
fastlane	Enables Fastlane parameters for 24GHz.
client-load-based	Enables client load-based EDCA configuration for 802.11 radios.
custom-voice	Enables custom voice EDCA parameters.
optimized-video-voice	Enables EDCA voice- and video-optimized profile parameters. Choose this option when both voice and video services are deployed on your network.
optimized-voice	Enables EDCA voice-optimized profile parameters. Choose this option when voice services other than SpectraLink are 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.
wmm-default	Enables the Wi-Fi Multimedia (WMM) default parameters. Choose this option when voice or video services are not deployed on your network.

Command Default

wmm-default

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
10.3	The **custom-voice** keyword was removed for Cisco 5700 Series WLC.
Cisco IOS XE Bengaluru 17.5.1	The **client-load-based** keyword was added.

This example shows how to enable SpectraLink voice priority parameters:

```
Device(config)# ap dot11 24ghz edca-parameters svp-voice
```

ap dot11 load-balancing denial

To configure the load balancing denial count, use the **ap dot11 load-balancingdenial**command. To disable load balancing denial count, use the **no** form of the command.

ap dot11 {**24ghz** | **5ghz**} **load-balancingdenial** *count*

Syntax Description

count	Load balancing denial count.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Example

The following example shows how to configure the load balancing denial count:

```
Device# configure terminal
Device(config)# ap dot11 5ghz load-balancing denial 10
```

ap dot11 load-balancing window

To configure the number of clients for the aggressive load balancing client window, use the **ap dot11 load-balancingwindow**command. To disable the client count, use the **no** form of the command.

ap dot11 {**24ghz** | **5ghz**} **load-balancingwindow** *clients*

Syntax Description

clients	Number of clients. Valid range is from 0 to 20.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Example

The following example shows how to configure the number of clients for the aggressive load balancing client window:

```
Device# configure terminal
Device(config)# ap dot11 5ghz load-balancing window 10
```

ap dot11 rf-profile

To configure an RF-Profile for a selected band, use the **ap dot11 rf-profile** command. To delete an RF-Profile, use the **no** form of this command.

ap dot11 { **24ghz** | **5ghz** | **6ghz** } **rf-profile** *profile name*

Syntax Description

24ghz	Displays the 2.4-GHz band
5ghz	Displays the 5-GHz band
6ghz	Displays the 6-GHz band
profile name	Name of the RF profile

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.
	6-GHz band was introduced in Cisco IOS XE Cupertino 17.7.1.

Usage Guidelines

None

This example shows how to configure an RF profile for a selected band.

```
Device#ap dot11 24GHz rf-profile doctest
```

ap dot11 rrm

To configure basic and advanced radio resource management settings for 802.11 devices, use the **ap dot11 rrm** command.

ap dot11 {**24ghz** | **5ghz**} **rrm** {**ccx location-measurement** *sec* | **channel** {**cleanair-event** | **dca** | **device** | **foreign** | **load** | **noise** | **outdoor-ap-dca**} | **coverage** {**data fail-percentage** *pct* | **data packet-count** *count* | **data rssi-threshold** *threshold*} | **exception global** *percentage* | **level global** *number* | **voice** {**fail-percentage** *percentage* | **packet-count** *number* | **rssi-threshold** *threshold*}}

Syntax Description

ccx	Configures Advanced (RRM) 802.11 CCX options.
location-measurement	Specifies 802.11 CCX Client Location Measurements in seconds. The range is between 10 and 32400 seconds.
channel	Configure advanced 802.11-channel assignment parameters.
cleanair-event	Configures cleanair event-driven RRM parameters.
dca	Configures 802.11-dynamic channel assignment algorithm parameters.
device	Configures persistent non-WiFi device avoidance in the 802.11-channel assignment.
foreign	Enables foreign AP 802.11-interference avoidance in the channel assignment.
load	Enables Cisco AP 802.11-load avoidance in the channel assignment.
noise	Enables non-802.11-noise avoidance in the channel assignment.
outdoor-ap-dca	Configures 802.11 DCA list option for outdoor AP.
coverage	Configures 802.11 coverage Hole-Detection.

data fail-percentage *pct*	Configures 802.11 coverage failure-rate threshold for uplink data packets. The range is between 1 and 100
data packet-count *count*	Configures 802.11 coverage minimum-failure-count threshold for uplinkdata packets.
data rssi-threshold *threshold*	Configures 802.11 minimum-receive-coverage level for voice packets.
exception global *percentage*	Configures 802.11 Cisco APs coverage-exception level. The range is between 0 and 100 percent.
level global *number*	Configures 802.11 Cisco AP client-minimum-exception level between 1 and 75 clients.
voice	Configures 802.11 coverage Hole-Detection for voice packets.
fail-percentage *percentage*	Configures 802.11 coverage failure rate threshold for uplink voice packets.
packet-count *number*	Configures 802.11 coverage minimum-uplink-failure count threshold for voice packets.
rssi-threshold *threshold*	Configures 802.11 minimum receive coverage level for voice packets.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

This command applies for both 802.11a and 802.11b bands. But the appropriate commands must be chosen for configuring the parameter.

This example shows how to configure various RRM settings.

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#ap dot11 5ghz rrm ?
```

```
ccx             Configure Advanced(RRM) 802.11a CCX options
channel         Configure advanced 802.11a channel assignment parameters
coverage        802.11a Coverage Hole Detection
group-member    Configure members in 802.11a static RF group
group-mode      802.11a RF group selection mode
logging         802.11a event logging
monitor         802.11a statistics monitoring
ndp-type        Neighbor discovery type Protected/Transparent
profile         802.11a performance profile
tpc-threshold   Configures the Tx Power Control Threshold used by RRM for auto
                power assignment
txpower         Configures the 802.11a Tx Power Level
```

ap dot11 rrm channel

To enable radio resource management channel for 2.4 GHz and 5GHz devices, use the **ap dot11 rrm channel** command. To disable the radio resource mangement for 2.4 GHz and 5 GHz devices, use the **no** form of the command.

ap dot11 {**24ghz** | **5ghz**} **rrm channel** {**cleanair-event** | **dca** | **device** | **foreign** | **load** | **noise**}
no ap dot11 {**24ghz** | **5ghz**} **rrm channel** {**cleanair-event** | **dca** | **device** | **foreign** | **load** | **noise**}

Syntax Description

cleanair-event	Specifies the cleanair event-driven RRM parameters
dca	Specifies the 802.11 dynamic channel assignment algorithm parameters
device	Specifies the persistent non-WiFi device avoidance in the 802.11-channel assignment.
foreign	Enables foreign AP 802.11-interference avoidance in the channel assignment.
load	Enables Cisco AP 802.11-load avoidance in the channel assignment.
noise	Enables non-802.11-noise avoidance in the channel assignment.

Command Default

None.

Command Modes

Interface configuration.

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

None.

This example shows all the parameters available for **Channel**.

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#ap dot11 24ghz rrm channel ?
  cleanair-event  Configure cleanair event-driven RRM parameters
  dca             Config 802.11b dynamic channel assignment algorithm
                  parameters
  device          Configure persistent non-WiFi device avoidance in the 802.11b
                  channel assignment
  foreign         Configure foreign AP 802.11b interference avoidance in the
                  channel assignment
  load            Configure Cisco AP 802.11b load avoidance in the channel
                  assignment
  noise           Configure 802.11b noise avoidance in the channel assignment
```

ap dot11 rrm channel cleanair-event

To configure CleanAir event-driven Radio Resource Management (RRM) parameters for all 802.11 Cisco lightweight access points, use the **ap dot11 rrm channel cleanair-event** command. When this parameter is configured, CleanAir access points can change their channel when a source of interference degrades the operations, even if the RRM interval has not expired yet.

ap dot11 {**24ghz** | **5ghz**} **rrm channel** {**cleanair-event sensitivity** *value*}

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
sensitivity	Sets the sensitivity for CleanAir event-driven RRM.
value	Sensitivity value. You can specify any one of the following three optional sensitivity values: • **low**—Specifies low sensitivity. • **medium**—Specifies medium sensitivity. • **high**—Specifies high sensitivity.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

This example shows how to set the high sensitivity for CleanAir event-driven RRM:

```
Device(config)# ap dot11 24ghz rrm channel cleanair-event sensitivity high
```

ap dot11 rrm channel dca

To configure Dynamic Channel Assignment (DCA) algorithm parameters on 802.11 networks, use the **ap dot11 rrm channel dca** command.

ap dot11 {**24ghz** | **5ghz**} **rrm channel dca** {*channel_number* | **anchor-time** *value* | **global** {**auto** | **once**} | **interval** *value* | **min-metric** *value* | **sensitivity** {**high** | **low** | **medium**}}

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
channel_number	Channel number to be added to the DCA list. **Note** The range is from 1 to 14.
anchor-time	Specifies the anchor time for DCA.
value	Hour of time between 0 and 23. These values represent the hour from 12:00 a.m. to 11:00 p.m.
global	Specifies the global DCA mode for the access points in the 802.11 networks.
auto	Enables auto-RF.
once	Enables one-time auto-RF.
interval	Specifies how often the DCA is allowed to run.
value	Interval between the times when DCA is allowed to run. Valid values are 0, 1, 2, 3, 4, 6, 8, 12, or 24 hours. 0 is 10 minutes (600 seconds). Default value is 0 (10 minutes).
min-metric	Specifies the DCA minimum RSSI energy metric.
value	Minimum RSSI energy metric value from –100 to –60.
sensitivity	Specifies how sensitive the DCA algorithm is to environmental changes (for example, signal, load, noise, and interference) when determining whether or not to change channels.
high	Specifies that the DCA algorithm is not particularly sensitive to environmental changes. See the “Usage Guidelines” section for more information.
low	Specifies that the DCA algorithm is moderately sensitive to environmental changes. See the “Usage Guidelines” section for more information.
medium	Specifies that the DCA algorithm is highly sensitive to environmental changes. See the “Usage Guidelines” section for more information.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

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. The table below explains the possible error codes for failed calls.

Table 4: DCA Sensitivity Threshold

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

This example shows how to configure the device to start running DCA at 5 pm for the 2.4 GHz band:

```
Device(config)# ap dot11 24ghz rrm channel dca anchor-time 17
```

This example shows how to set the DCA algorithm to run every 10 minutes for the 2.4 GHz band:

```
Device(config)# ap dot11 24ghz rrm channel dca interval 0
```

This example shows how to configure the value of DCA algorithm's sensitivity to low on the 2.4 GHz band:

```
Device(config)# ap dot11 24ghz rrm channel dca sensitivity low
```

ap dot11 rrm channel-update mesh

To initiate update of the 802.11a, 802.11b, and 802.11 6GHz channel selection for every mesh Cisco AP, use the **ap dot11** {**24ghz** | **5ghz** | **6ghz**} **rrm channel-update mesh**

AP

ap dot11 { **24ghz** | **5ghz** | **6ghz** } **rrm channel-update mesh**

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Cupertino 17.9.1	This command was introduced.

Example

The example shows how to initiate update of the 802.11a, 802.11b, and 802.11 6GHz channel selection for every mesh Cisco AP:

```
Device# ap dot11 5ghz rrm channel-update mesh
```

ap dot11 rrm channel-update mesh bridge-group

To initiate the update of the 802.11, 802.11a, or 802.11b channel selection for mesh AP in the bridge group, use the **ap dot11** {**24ghz** | **5ghz** | **6ghz**} **channel-update mesh bridge-group**

ap dot11 { **24ghz** | **5ghz** | **6ghz** } **rrm channel-update mesh channel-update mesh bridge-group** *bridge-group-name*

Syntax Description

bridge-group-name	Specifies the name of the bridge group.

Command Default

None

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Cupertino 17.9.1	This command was introduced.

Example

This example shows how to initiate the update of the 802.11, 802.11a, or 802.11b channel selection for mesh AP in the bridge group:

```
Device# ap dot11 5ghz rrm channel-update mesh bridge-group cisco-bridge-group
```

ap dot11 rrm channel dca chan-width

To configure channel width for IEEE 802.11 radios, use the **ap dot11 rrm channel dca chan-width** command.

ap dot11 {**24ghz** | **5ghz**} **rrm channel dca chan-width** {**160** | **20** | **40** | **80** | **80+80** | **best** | **width-max**}

Syntax Description

160	160 MHz.
20	20 MHz.
40	40 MHz.
80	80 MHz.
80+80	80+80 MHz.
best	Best channel width.
width-max	Maximum best channel width allowed for dynamic bandwidth selection.

Command Default

None

Command Modes

Global Configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Usage Guidelines

Example

The following example shows how to configure channel width for IEEE 802.11 radios.

```
Device(config)# ap dot11 5ghz rrm channel dca chan-width 160
```

ap dot11 rrm coverage

To enable 802.11 coverage hole detection, use the **ap dot11 rrm coverage** command.

ap dot11 {**24ghz** | **5ghz**} **rrm coverage** [**data** {**fail-percentage** *percentage* | **packet-count** *count* | **rssi-threshold** *threshold*} | **exceptional global** *value* | **level global** *value* | **voice** {**fail-percentage** *percentage* | **packet-count** *packet-count* | **rssi-threshold** *threshold*}]

Syntax Description

data	Specifies 802.11 coverage hole-detection data packets.
fail-percentage *percentage*	Specifies 802.11 coverage failure-rate threshold for uplink data packets. The range is between 1 and 100
packet-count *count*	Specifies 802.11 coverage minimum-failure-count threshold for uplink data packets.
rssi-threshold *threshold*	Specifies 802.11 minimum-receive-coverage level for voice packets.
exceptional global *value*	Specifies 802.11 Cisco APs coverage-exception level. The range is between 0 and 100 percent.
level global *value*	Specifies 802.11 Cisco AP client-minimum-exception level between 1 and 75 clients.
voice	Specifies 802.11 coverage Hole-Detection for voice packets.
fail-percentage *percentage*	Specifies 802.11 coverage failure rate threshold for uplink voice packets.
packet-count *packet-count*	Specifies 802.11 coverage minimum-uplink-failure count threshold for voice packets.
rssi-threshold *threshold*	Specifies 802.11 minimum receive coverage level for voice packets.

Command Default

None.

Command Modes

Interface configuration.

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

If you enable coverage hole-detection, the device 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 **ap dot11 {24ghz | 5ghz} rrm coverage packet-count** and **ap dot11 {24ghz | 5ghz} rrm coverage fail-percentage** commands for a 5-second period, the client is considered to be in a pre-alarm condition. The device 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

ap dot11 {24ghz | 5ghz} rrm coverage level-global and **ap dot11 {24ghz | 5ghz} rrm coverage exceptional-global** commands over a 90-second period. The device determines whether the coverage hole can be corrected and, if appropriate, mitigate the coverage hole by increasing the transmit power level for that specific access point.

This example shows how to set the RSSI-threshold for data in 5-GHz band.

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#ap dot11 5ghz rrm coverage data rssi-threshold -80
```

ap dot11 rrm group-member

To configure members in an 802.11 static RF group, use the **ap dot11 rrm group-member** command. To remove members from 802.11 RF group, use the **no** form of this command.

ap dot11 {**24ghz** | **5ghz**} **rrm group-member** *controller-name controller-ip*
no ap dot11 {**24ghz** | **5ghz**} **rrm group-member** *controller-name controller-ip*

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
controller-name	Name of the device to be added.
controller-ip	IP address of the device to be added.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

This example shows how to add a device in the 5 GHz band RF group:

```
Device(config)# ap dot11 5ghz rrm group-member cisco-controller 192.0.2.54
```

ap dot11 rrm group-mode

To set the 802.11 automatic RF group selection mode on, use the **ap dot11 rrm group-mode** command. To set the 802.11 automatic RF group selection mode off, use the **no** form of this command.

ap dot11 { **5ghz** | **24ghz** | **6ghz** } **rrm group-mode** { **auto** | **leader** | **off** | **restart** }
no ap dot11 {**5ghz** | **24ghz**} **rrm group-mode**

Syntax Description

5ghz	Specifies the 2.4-GHz band.
24ghz	Specifies the 5-GHz band.
6ghz	Specifies the 6-GHz band.
auto	Sets the 802.11 RF group selection to automatic update mode.
leader	Sets the 802.11 RF group selection to static mode, and sets this device as the group leader.
off	Sets the 802.11 RF group selection to off.
restart	Restarts the 802.11 RF group selection.

Command Default

auto

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
Cisco IOS XE Cupertino 17.7.1	This command was modified to include the 6-GHz band.

This example shows how to turn the auto RF group selection mode on the 5 GHz band:

```
Device(config)# ap dot11 5ghz rrm group-mode auto
```

ap dot11 rrm logging

To configure report log settings on supported 802.11 networks, use the **ap dot11 rrm logging** command.

ap dot11 {**24ghz** | **5ghz**} **rrm logging** {**channel** | **coverage** | **foreign** | **load** | **noise** | **performance** | **txpower**}

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
channel	Turns the channel change logging mode on or off. The default mode is off (Disabled).
coverage	Turns the coverage profile logging mode on or off. The default mode is off (Disabled).
foreign	Turns the foreign interference profile logging mode on or off. The default mode is off (Disabled).
load	Turns the load profile logging mode on or off. The default mode is off (Disabled).
noise	Turns the noise profile logging mode on or off. The default mode is off (Disabled).
performance	Turns the performance profile logging mode on or off. The default mode is off (Disabled).
txpower	Turns the transit power change logging mode on or off. The default mode is off (Disabled).

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

This example shows how to turn the 5 GHz logging channel selection mode on:

```
Device(config)# ap dot11 5ghz rrm logging channel
```

This example shows how to turn the 5 GHz coverage profile violation logging selection mode on:

```
Device(config)# ap dot11 5ghz rrm logging coverage
```

This example shows how to turn the 5 GHz foreign interference profile violation logging selection mode on:

```
Device(config)# ap dot11 5ghz rrm logging foreign
```

This example shows how to turn the 5 GHz load profile logging mode on:

```
Device(config)# ap dot11 5ghz rrm logging load
```

This example shows how to turn the 5 GHz noise profile logging mode on:

```
Device(config)# ap dot11 5ghz rrm logging noise
```

This example shows how to turn the 5 GHz performance profile logging mode on:

```
Device(config)# ap dot11 5ghz rrm logging performance
```

This example shows how to turn the 5 GHz transmit power change mode on:

```
Device(config)# ap dot11 5ghz rrm logging txpower
```

ap dot11 rrm monitor

To Configure monitor settings on the 802.11 networks, use the **ap dot11 rrm monitor** command.

ap dot11 {**24ghz** | **5ghz**} **rrm monitor** {**channel-list** | {**all** | **country** | **dca**} | **coverage** | **load** | **noise** | **signal**} *seconds*

Syntax Description

24ghz	Specifies the 802.11b parameters.
5ghz	Specifies the 802.11a parameters.
channel-list all	Monitors the noise, interference, and rogue monitoring channel list for all channels.
channel-list country	Monitors the noise, interference, and rogue monitoring channel list for the channels used in the configured country code.
channel-list dca	Monitors the noise, interference, and rogue monitoring channel list for the channels used by automatic channel assignment.
coverage	Specifies the coverage measurement interval.
load	Specifies the load measurement interval.
noise	Specifies the noise measurement interval.
signal	Specifies the signal measurement interval.
rssi-normalization	Configure RRM Neighbor Discovery RSSI Normalization.
seconds	Measurement interval time from 60 to 3600 seconds.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

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

```
Device(config)# ap dot11 24ghz rrm monitor channel-list country
```

This example shows how to set the coverage measurement interval to 60 seconds:

```
Device(config)# ap dot11 24ghz rrm monitor coverage 60
```

ap dot11 rrm ndp-type

To configure the 802.11 access point radio resource management neighbor discovery protocol type, use the **ap dot11 rrm ndp-type** command.

ap dot11 { **24ghz** | **5ghz** | **6ghz** } **rrm ndp-type** { **protected** | **transparent** }

Syntax Description

24ghz	Specifies the 2.4-GHz band.
5ghz	Specifies the 5-GHz band.
6ghz	Specifies the 6-GHz band.
protected	Specifies the Tx RRM protected (encrypted) neighbor discovery protocol.
transparent	Specifies the Tx RRM transparent (not encrypted) neighbor discovery protocol.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
Cisco IOS XE Cupertino 17.7.1	This command was modified with the introduction of the 6-GHz band.

Usage Guidelines

Before you configure the 802.11 access point RRM neighbor discovery protocol type, ensure that you have disabled the network by entering the **ap dot11** {**24ghz | 5ghz | 6ghz**} **shutdown** command.

This example shows how to enable the 802.11a access point RRM neighbor discovery protocol type as protected:

```
Device(config)# ap dot11 5ghz rrm ndp-type protected
```

ap dot11 rrm tpc-threshold

To configure the tx-power control threshold used by RRM for auto power assignment, use the **ap dot11 rrm tpc-threshold** command. To disable, use the **no** form of the command.

ap dot11 {**24ghz** | **5ghz**} **rrm tpc-threshold** *value*
no ap dot11 {**24ghz** | **5ghz**} **rrm tpc-threshold**

Syntax Description

value	Specifies the power value. The range is between -80 and -50.

Command Default

None.

Command Modes

Interface configuration.

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

None.

This example shows how to configure the tx-power control threshold used by RRM for auto power assignment.

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#ap dot11 5ghz rrm tpc-threshold -60
```

ap dot11 rrm txpower

To configure the 802.11 tx-power level, use the **ap dot11 rrm txpower** command. To disable the 802.11 tx-power level, use the **no** form of the command.

ap dot11 {**24ghz** | **5ghz**} **rrm txpower** {**auto** | **max** *powerLevel* | **min** *powerLevel* | **once***power-level*}
noap dot11 {**24ghz** | **5ghz**} **rrm txpower** {**auto** | **max** *powerLevel* | **min** *powerLevel* | **once***power-level*}

Syntax Description

auto	Enables auto-RF.
max *powerLevel*	Configures maximum auto-RF tx power. The range is between -10 to -30.
min *powerLevel*	Configures minimum auto-RF tx power. The range is between -10 to -30.
once	Enables one-time auto-RF.

Command Default

None.

Command Modes

Interface configuration.

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
	The **no** form of the command is introduced.

Usage Guidelines

None.

This example shows how to enables auto-RF once.

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#ap dot11 5ghz rrm txpower once
```

ap dot11 rrm txpower

To configure the 802.11 tx-power level, use the **ap dot11 rrm txpower** command. To disable the 802.11 tx-power level, use the **no** form of the command.

ap dot11 {**24ghz** | **5ghz**} **rrm txpower** {**auto** | **max** *powerLevel* | **min** *powerLevel* | **once***power-level*}
noap dot11 {**24ghz** | **5ghz**} **rrm txpower** {**auto** | **max** *powerLevel* | **min** *powerLevel* | **once***power-level*}

Syntax Description

auto	Enables auto-RF.
max *powerLevel*	Configures maximum auto-RF tx power. The range is between -10 to -30.
min *powerLevel*	Configures minimum auto-RF tx power. The range is between -10 to -30.
once	Enables one-time auto-RF.

Command Default

None.

Command Modes

Interface configuration.

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
	The **no** form of the command is introduced.

Usage Guidelines

None.

This example shows how to enables auto-RF once.

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#ap dot11 5ghz rrm txpower once
```

ap dot15 shutdown

To configure the global dot 15 radio parameters, use the **ap dot15 shutdown** command. To disable the configuration, use the no form of command.

ap dot15 shutdown

no ap dot15 shutdown

Syntax Description

dot15	Configures for global Dot15 radio parameters.
shutdown	Disable Dot15 radio for all APs .

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.3.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows how to configure the global dot 15 radio parameters:

```
Device(config)# ap dot15 shutdown
```

ap file-transfer https port

To configure the custom port number for AP image download over HTTPS, use the **ap file-transfer https port** command. To remove the the custom port number, use the **no** form of this command.

ap file-transfer https port *port-number*

Syntax Description

port-number	Custom port number for the file transfer. The valid values range from 0 to 65535, with a default of 8443.

Command Default

Default port is 8443.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Dublin 17.11.1	This command was introduced.

Usage Guidelines

Do not use port 443 for AP file transfers because it is the default port that is used for other HTTPS requests. Also, avoid configuring standard and well-known ports because the configuration might fail.

Examples

The following example shows how to configure the custom port number for AP image download over HTTPS:

```
Device# configure terminal
Device(config)# ap file-transfer https port 8443
```

ap filter

To configure the AP filter and set the priority, use the **ap filter** command.

ap filter { { **name** *filter-name* } **type** { **priming** | | **tag** } | { **priority** *priority-number* | **filter-name** *filter-name* } }

Syntax Description

Parameter	Description
priority	Set the priority for a named filter.
priority-number	The valid AP filter priority range is 0 to 1023.
filter-name	Enter the name for the ap filter.
type	Type of filter.
priming	Filter to prime APs. This filter is always persistent on the AP.
tag	Filter to assign AP Tags. Tag filter may be persistent based on tag persistence on the global configuration.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.
Cisco IOS XE Dublin 17.10.1	This command was modified. The **priming** keyword was introduced.

Examples

The following example shows how to create a ap filter and set the priority to this filter:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap filter name test-filter
Device(config)# ap filter name test-filter type priming
Device(config)# ap filter priority 12 filter-name test-filter
```

ap fra

To configure flexible radio assignment (FRA) and its parameters, use the **ap fra** command.

ap fra[**interval** *no-of-hours* | **sensitivity** {**high** | **low** | **medium** } | **sensor-threshold** {**balanced** | **client-preferred** | **client-priority** | **sensor-preferred** | **sensor-priority** } | **service-priority** {**coverage** | **service-assurance**}]

Syntax Description

interval *no-of-hours*	Enter the number of hours for the FRA interval. Valid range is 1 to 24 hours.
sensitivity {**high** | **low** | **medium**}	Configures the FRA coverage overlap sensitivity as high, low, or medium.
sensor-threshold {**balanced** | **client-preferred** | **client-priority** | **sensor-preferred** | **sensor-priority**}	Configures FRA sensor threshold to one of the available options.
service-priority {**coverage** | **service-assurance**}	Configures FRA service priority to Coverage or Service Assurance.

Command Default

None

Command Modes

config

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Usage Guidelines

Ensure that the RF group leader for 802.11b/g and 802.11a bands are same across RF domain and make sure that the RF group leader has FRA enabled.

Examples

The following example show how to configure the FRA interval to 8 hours:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap fra interval 8
```

ap fra 5-6ghz

To enable Flexible Radio Assignment (FRA) 5/6GHz on all Cisco APs, use the **ap fra 5-6ghz** command in the global configuration mode. Use the **no** form of this command to disable the feature.

ap fra 5-6ghz

no ap fra 5-6ghz

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global Configuration

Command History

Release	Modification
Cisco IOS XE Cupertino 17.9.1	This command was introduced.

Example

This example shows how to enable Flexible Radio Assignment (FRA) 5/6GHz on all Cisco APs:

```
Device(config)# ap fra 5-6ghz
Device(config)# no ap fra 5-6ghz
```

ap fra 5-6ghz freeze

To enable 5-6-GHz Flexible Radio Assignment (FRA) freeze on all Cisco APs, use the **ap fra 5-6ghz freeze** command in the global configuration mode. Use the **no** form of this command to disable the feature.

ap fra 5-6ghz freeze

no ap fra 5-6ghz freeze

Syntax Description

There are no arguments for this command.

Command Default

None

Command Modes

Global Configuration

Command History

Release	Modification
Cisco IOS XE Cupertino 17.9.1	This command was introduced.

Example

This example shows how to enable 5-6-GHz Flexible Radio Assignment (FRA) freeze on all Cisco APs:

```
Device# ap fra 5-6ghz freeze
Device# no ap fra 5-6ghz freeze
```

ap fra 5-6ghz interval

To configure the Flexible Radio Assignment (FRA) 5/6-GHz interval in hours, use the **ap fra 5-6ghz interval** command.

ap fra 5-6ghz interval *number-of-hours*

Syntax Description

number-of-hours	Specifies the FRA 5/6-GHz interval in hours. The value range is between 1 to 24 hours.

Command Default

None

Command Modes

Global Configuration

Command History

Release	Modification
Cisco IOS XE Cupertino 17.9.1	This command was introduced.

Example

This example shows how to configure the Flexible Radio Assignment (FRA) 5/6-GHz interval in hours:

```
Device(config)# ap fra 5-6ghz interval 12
```

ap geolocation derivation ranging

To configure the geolocation derivation ranging, use the **ap geolocation derivation ranging** command. To disable the geolocation derivation ranging feature, use the **no** form of this command.

ap geolocation derivation ranging

no ap geolocation derivation ranging

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Cisco IOS XE Dublin 17.12.1	This command was introduced.

Example

This example shows how to configure an AP geolocation derivation ranging:

```
Device# configure terminal
Device(config)# ap geolocation derivation ranging
```

ap geolocation ranging all accurate

To enable accurate ranging on all APs using 5-GHz or 6-GHz bands, use the **ap geolocation ranging all accurate** command.

Syntax Description

5ghz	Enable accurate ranging using 5-GHz band on all APs.
6ghz	Enable accurate ranging using 6-GHz band on all APs.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Dublin 17.12.1	This command was introduced.
Cisco IOS XE Dublin 17.13.1	This command was modified by adding the keywords **5ghz** and **6ghz**.

Usage Guidelines

Client connections could be disrupted.

Example

This example shows how to enable accurate ranging on all APs using 5-GHz or 6-GHz bands:

```
Device# ap geolocation ranging all accurate 5ghz
```

ap geolocation ranging site accurate

To enable accurate ranging on APs under configured site-tag using 5-GHz or 6-GHz bands, use the **ap geolocation ranging site** *site-tag-name* **accurate** command.

ap geolocation ranging site *site-tag-name* **accurate** [**5ghz** | **6ghz**]

Syntax Description

site-tag-name	Specifies the site-tag name.
5ghz	Enable accurate ranging using 5-GHz band on all APs.
6ghz	Enable accurate ranging using 6-GHz band on all APs.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Dublin 17.12.1	This command was introduced.
Cisco IOS XE Dublin 17.13.1	This command was modified by adding the keywords **5ghz** and **6ghz**.

Usage Guidelines

Client connections could be disrupted.

Example

This example shows how to enable accurate ranging on APs under configured site-tag using 5-GHz or 6-GHz bands:

```
Device# ap geolocation ranging site site-tag-name accurate 5ghz
```

ap hyperlocation

To configure hyperlocation and related parameters, use the **ap hyperlocation** command. To disable hyperlocation and related parameters, use the **no** form of this command.

ap hyperlocation [**ble-beacon** {*beacon-id* | **interval** *interval-value*} | **threshold** {**detection** *value-in-dBm* | **reset** *value-btwn-0-99* | **trigger** *value-btwn-1-100*}]
[no] ap hyperlocation [**ble-beacon** {*beacon-id* | **interval** *interval-value*} | **threshold** {**detection** *value-in-dBm* | **reset** *value-btwn-0-99* | **trigger** *value-btwn-1-100*}]

Syntax Description

ble-beacon	Enables BLE beacon parameters.
beacon-id	BLE beacon ID. The range is from 1 to 4.
interval	Sets the BLE beacon interval.
interval-value	BLE beacon interval value, in hertz. The range is from 1 to 10. The default is1.
threshold detection *value-in-dBm*	Sets threshold to filter out packets with low RSSI. The **[no]** form of the command resets the threshold to its default value.
threshold reset *value-btwn-0-99*	Resets value in scan cycles after trigger. The **[no]** form of the command resets the threshold to its default value.
threshold trigger *value-btwn-1-100*	Sets the number of scan cycles before sending a BAR to clients. The **[no]** form of the command resets the threshold to its default value. **Note** Ensure that the hyperlocation threshold reset value is less than the threshold trigger value.

Command History

Release	Modification
Cisco IOS XE Denali 16.2.1	This command was introduced.
Cisco IOS XE Denali 16.3.1	This command was modified. The **ble-beacon** keyword was added.

ap image

To configure an image on access points or move access points to another controller, use the **ap image** command.

ap image { **predownload** | **reset** | **swap** | **move destination** *controller-name* { *controller-ipv4-addr controller-ipv6-addr* } [*report-name*] }

Syntax Description

predownload	Instructs all the access points to start predownloading an image.
reset	Instructs all the access points to reboot.
swap	Instructs all the access points to swap the image.
move	Moves access points to the specified destination controller without swapping the AP image or resetting the access points.
destination *controller-name controller-ip* [*report-name*]	Specifies the name and wireless management IP address of the destination controller. The optional *report-name* specifies an existing AP upgrade report whose iterations are used to move the access points.

Usage Guidelines

Use **move** in an N+1 hitless rolling upgrade to move access points back to the parent controller after the controller image has been activated and committed. This command does not perform an image swap or reset the access points.

Establish a mobility tunnel between the controllers before using this command. The destination controller should run the same AP image.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

This example shows how to predownload an image to all access points:

```
Device# ap image predownload
```

This example shows how to reboot all access points:

```
Device# ap image reset
```

This example shows how to swap the access point's primary and secondary images:

```
Device# ap image swap
```

This example shows how to move access points to a destination controller without swapping the AP image or resetting the access points:

```
Device# ap image move destination mywlc 1.2.3.4 myreport
```

ap image site-filter

To upgrade an access point (AP) image using software maintenance update (SMU) based on a site filter, use the **ap image site-filter** command.

ap image site-filter file *file-name* **any remove-all** { **add** *site-tag* | **apply** | **clear** | **remove** *site-tag* }

Syntax Description

file-name	SMU image name.
site-tag	Site tag name.
add	Adds a site in the site filter.
apply	Predownloads the AP image and performs rolling AP upgrade in staggered manner.
clear	Clears the existing site filters.
remove	Removes a site from the site filter.
any	
remove-all	

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.
Cisco IOS XE Cupertino 17.9.1	This command was modified by adding the keywords **any** and **remove-all**.

Example

The following example shows how to upgrade an AP image using the SMU, based on a site filter:

```
Device# ap image site-filter file vwlc_apsp_16.11.1.0_74.bin add bgl18
```

ap image upgrade

To instruct all the APs to start image upgrade, use the **ap image upgrade** command.

ap image upgrade [**abort** | **destination** *controller-name* {*controller-ipv4-addr controller-ipv6-addr* } | **dry-run**]

Syntax Description

abort	Cancels AP image upgrade.
destination *controller-name* {*controller-ipv4-addr* | *controller-ipv6-addr*}	Instructs all the APs to associate with the destination controller whose name and IP address you must enter.
dry-run	Runs the rolling AP image upgrade in dry-run mode.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to cancel an AP image upgrade:

```
Device# ap image upgrade abort
```

ap link-encryption

To enable Datagram Transport Layer Security (DTLS) data encryption for access points, use the **ap link-encryption** command. To disable the DTLS data encryption for access points, use the **no** form of this command.

ap link-encryption
no ap link-encryption

Syntax Description

This command has no keywords and arguments.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

This example shows how to enable data encryption for all the access points that are joined to the controller:

```
Device(config)# ap link-encryption
```

ap lsc-provision

To configure LSC provisioning on an AP, use the **ap lsc-provision** command. To remove the behavior of this command, use the **no** form of this command.

ap lsc-provision

no ap lsc-provision

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

configuration (config)

Command History

Release	Modification
Cisco IOS XE 17.17.1	This command was introduced.

Examples

This example shows how to configure LSC provisioning on an AP:

```
Device# configure terminal
Device(config)# ap lsc-provision
```

ap lsc-provision renew due-time

To renew AP LSCs automatically within the specified number of days, use the **ap lsc-provision renew due-time** command. To remove the behavior of this command, use the **no** form of this command.

ap lsc-provision renew due-time [*no-of-days*]
no ap lsc-provision renew due-time [*no-of-days*]

Syntax Description

due-time	Renew AP LSCs automatically within the specified number of days.
no-of-days	The valid range is from 5 to 60 days, with a default value of 30 days.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 17.17.1	This command was introduced.

Examples

This example shows how to renew AP LSCs automatically within the specified number of days:

```
Device# configure terminal
Device(config)# ap lsc-provision renew due-time 15
```

ap lsc-provision renew one-shot

To renew all AP LSCs in a single iteration, use the **ap lsc-provision renew one-shot** command. To remove the behavior of this command, use the **no** form of this command.



Note You cannot use one-shot and staggered renewal methods at the same time.

ap lsc-provision renew one-shot
no ap lsc-provision renew one-shot

Syntax Description

This command has no arguments or keywords.

Command Default

The one-shot AP LSC renewal feature is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 17.17.1	This command was introduced.

Examples

This example shows how to renew all AP LSCs in a single iteration:

```
Device# configure terminal
Device(config)# ap lsc-provision renew one-shot
```

ap lsc-provision renew staggered

To renew AP LSCs automatically in a staggered manner, use the **ap lsc-provision renew staggered** command. To remove the behavior of this command, use the **no** form of this command.

Note You cannot use one-shot and staggered renewal methods at the same time.

ap lsc-provision renew staggered timeout [*iteration-timeout-in-mins*]
no ap lsc-provision renew staggered timeout [*iteration-timeout-in-mins*]

Syntax Description

timeout	Represents the iteration timeout.
iteration-timeout-in-mins	Refers to the iteration timeout in minutes. The valid range is from 5 to 60 minutes.

Command Default

Staggered AP LSC renewal is enabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 17.17.1	This command was introduced.

Examples

This example shows how to renew AP LSCs automatically in a staggered manner:

```
Device# configure terminal
Device(config)# ap lsc-provision renew staggered timeout 20
```

ap lsc-provision renew schedular

To configure time schedule for auto-renewal within a maintenance window, use the **ap lsc-provision renew schedular** command. To remove the behavior of this command, use the **no** form of this command.

Note You must configure the calendar-profile definition beforehand. For more information, see **calender-profile name**.

ap lsc-provision renew schedular [*calendar-profile-name*]
no ap lsc-provision renew schedular [*calendar-profile-name*]

Syntax Description

calendar-profile-name	Calendar profile name.

Command Default

No scheduler is enabled by default.

When no scheduler is applied, the device auto-renews AP LSCs at 24-hour intervals.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 17.17.1	This command was introduced.

Examples

This example shows how to configure time schedule for auto-renewal within a maintenance window:

```
Device# configure terminal
Device(config)# ap lsc-provision renew schedular daily_calendar_profile
```

ap lsc renew due-time

To renew a specific site-tag AP that is set to expire within the specified time, use the **ap lsc renew due-time** command. To remove the behavior of this command, use the **no** form of this command.

ap lsc renew due-time *number-of-days* **site-tag** *site-tag-name*
no ap lsc renew due-time *number-of-days* **site-tag** *site-tag-name*

Syntax Description

number-of-days	The valid range is from 1 to 60 days.
site-tag-name	Name of the site tag.

Command Default

None

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE 17.17.1	This command was introduced.

Examples

This example shows how to renew a specific site-tag AP that is set to expire within the specified time:

```
Device# enable
Device# ap lsc renew due-time 20 site-tag site-tag-name1
```

ap name icap subscription ap rf spectrum

To configure spectrum analysis on an AP, use the **ap nameicap subscription ap rf spectrum** command. To disable spectrum analysis, use the **no** form of the command.

ap name *ap_name* **icap subscription ap rf spectrum { enable** | *slot }*

Syntax Description

enable	Enable the subscription.
slot	Configures the radio slots to collect RF spectrum measurements.
ap_name	AP name

Command Default

Disabled

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.2.1	This command was introduced.

Usage Guidelines

For the subscription to function, at least one radio slot must also be configured, having Cisco CleanAir enabled and operational state as up.

Example

The following example shows how to enable spectrum analysis on a AP:

```
Device# ap name 4800AP icap subscription ap rf spectrum enable
Device# ap name 4800AP icap subscription ap rf spectrum slot 0
Device# show ap name 4800AP icap subscription ap rf spectrum chassis active
```

ap name antenna band mode

To configure the antenna mode, use the **ap name***ap- name* **antenna-band-mode{ single | dual }** command.

ap name*ap-name* **antenna-band-mode** {**single** | **dual**}

Syntax Description

ap- name	Name of the Cisco lightweight access point.
antenna-band-mode	Instructs the access point to enable the band mode of antenna.

Command Default

None

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Example

This example shows how to configure the antenna band mode of access point.

```
Deviceap name <ap-name> antenna-band-mode single
```

ap name ble

To enable the able ltx state on the AP, use the **ap name** *ap name* **ble** command.

ap name *ap_name* **antena-band-mode {admin | ibeacon | interval | no-advertisement | sync | vibeacon}**

Syntax Description

ap name	AP Name
admin	Enables the ble ltx admin state.
ibeacon	Enables the BLE LTX iBeacon configuration.
interval	Enables the BLE LTX scan configuration interval.
no-advertisement	Enables the BLE LTX No Advertisement.
Sync	Enables the BLE LTX synchronize.
vibeacon	Enables the BLE LTX viBeacon configuration.

Command Default

Disabled

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Examples

The following example shows how to enable ble on the AP:

```
Device# ap name test ble
```

ap name clear-personal-ssid

To clear the personal SSID from a Cisco OfficeExtend Access Point (OEAP), use the **ap name clear-personal-ssid** command.

ap name *ap-name* **clear-personal-ssid**

Syntax Description

ap-name	AP name.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to clear the personal SSID from a Cisco OEAP:

```
Device# ap name my-oeap clear-personal-ssid
```

ap name controller

To configure the controller on the AP, use the **ap name** *ap name* **controller** command.

ap name *ap_name* **controller {primary | secondary | tertiary}** *name {A.B.C.D | X:X:X::XX}*

Syntax Description

ap name	AP Name
controller	Configures the controller.
primary	Configures the primary controller.
secondary	Configures the secondary controller.
tertiary	Configures the tertiary controller.
name	Specifies the name of the primary controller, secondary controller, or tertiary controller.
A.B.C.D	Specifies theIPv4 address of the primary controller, secondary controller, or tertiary controller.
X:X:X::XX	Specifies theIPv6 address of the primary controller, secondary controller, or tertiary controller.

Command Default

Disabled

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Examples

The following example shows how to configure the controller on the AP:

```
Device# ap name cisco-ap controller primary cisco-primary-controller 10.1.1.1
```

ap name core-dump

To configure a Cisco lightweight access point's memory core dump, use the **ap name core-dump** command. To disable a Cisco lightweight access point's memory core dump, use the **no** form of this command.

ap name *ap-name* **core-dump** *tftp-ip-addr filename* {**compress** | **uncompress**}
ap name *ap-name* [**no**] **core-dump**

Syntax Description

ap-name	Name of the access point.
tftp-ip-addr	IP address of the TFTP server to which the access point sends core dump files.
filename	Name that the access point used to label the core file.
compress	Compresses the core dump file.
uncompress	Uncompresses the core dump file.

Command Default

None

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

The access point must be able to reach the TFTP server before you can use this command.

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

```
Device# ap name AP2 core-dump 192.1.1.1 log compress
```

ap name country

To configure the country of operation for a Cisco lightweight access point, use the **ap name country** command.

ap name *ap-name* **country** *country-code*

Syntax Description

ap-name	Name of the Cisco lightweight access point.
country-code	Two-letter or three-letter country code.

Command Default

None

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

Cisco devices must be installed by a network administrator or qualified IT professional and the installer must select the proper country code. Following installation, access to the unit should be password protected by the installer to maintain compliance with regulatory requirements and to ensure proper unit functionality. See the related product guide for the most recent country codes and regulatory domains. Also, access point regulatory domains are defined during the access point manufacturing process. You can change the access point country code if the new country code matches a country that is valid within the access point regulatory domain. If you try to enter a country that is not valid to the access point regulatory domain, the command fails.

This example shows how to configure the Cisco lightweight access point's country code to DE:

```
Device# ap name AP2 country JP
```

ap name crash-file

To manage crash data and radio core files for the Cisco access point, use the **ap name crash-file** command.

ap name *ap-name* **crash-file** {**get-crash-data** | **get-radio-core-dump** {**slot 0** | **slot 1**}}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
get-crash-data	Collects the latest crash data for a Cisco lightweight access point.
get-radio-core-dump	Gets a Cisco lightweight access point's radio core dump
slot	Slot ID for Cisco access point.
0	Specifies Slot 0.
1	Specifies Slot 1.

Command Default

None

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

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

```
Device# ap name AP3 crash-file get-crash-data
```

This example shows how to collect the radio core dump for access point AP02 and slot 0:

```
Device# ap name AP02 crash-file get-radio-core-dump slot 0
```

ap name dot11 24ghz | 5ghz | 6ghz rrm channel update mesh

To trigger the RRM DCA for a specific AP, use the **ap name** *cisco-ap-name* **dot11** {**24ghz** | **5ghz** | **6ghz**} **rrm channel update mesh**

ap name *cisco-ap-name* **dot11** { **24ghz** | **5ghz** | **6ghz** } **rrm channel update mesh**

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Cupertino 17.9.1	This command was introduced.

Example

This example shows how to trigger the RRM DCA for a specific AP:

```
Device# ap name Cisco-ap-name dot11 5ghz rrm channel update mesh
```

ap name dot11 24ghz slot 0 SI

To enable Spectrum Intelligence (SI) for the dedicated 2.4-GHz radio hosted on slot 0 for a specific access point, use the **ap name dot11 24ghz slot 0 SI** command.

ap name *ap-name* **dot11** { **24ghz** | **5ghz** | **dual-band** | **rx-dual-band** } **slot** *slot ID* **SI**

Syntax Description

ap_name	Name of the Cisco Access Point.
slot 0	Enables Spectrum Intelligence (SI) for the dedicated 2.4-GHz radio hosted on slot 0 for a specific access point. Here, 0 refers to the Slot ID.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Example

The following example shows how to configure Spectrum Intelligence of an AP.

```
Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 SI
```

ap name dot11 24ghz slot antenna

To configure the 802.11b antenna hosted on slot 0, use the **ap name dot11 24ghz slot antenna** command.

ap name *ap-name***dot1124ghzslot 0antenna** { **ext-ant-gain** *antenna-gain-value* | **selection** [**internal** | **external** }

Syntax Description

ap-name	Name of the AP.
24ghz	Configures 802.11b parameters.
slot	Sets the slot ID for the Cisco Access Point.
antenna	Configures the 802.11b Antenna.
ext-ant-gain	Configures the 802.11b External Antenna Gain. The value range is 0 - 4294967295. Enter External Antenna Gain value in multiple of .5 dBi units (i.e. An integer value 4 means 4 x 0.5 = 2 dBi of gain)
selection	Configure the 802.11b Antenna selection (internal/external)

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Usage Guidelines

Example

The following example shows how to configure the channel width of an AP.

```
Device# ap name ax1 dot11 24ghz slot 0 antenna selection external
```

ap name dot11 24ghz slot beamforming

To configures beamforming for the 2.4-GHz radio hosted on slot 0 for a specific access point, use the **ap name dot11 24ghz slot beamforming** command.

ap name *ap-name***dot1124ghzslot 0beamforming**

Syntax Description

beamforming	Enable 802.11b tx beamforming - 5 GHz

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Usage Guidelines

Example

The following example shows how to configure beamforming of an AP.

```
Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 beamforming
```

ap name dot11 24ghz slot channel

To configure advanced 802.11 channel assignment parameters for Cisco AP, use the **ap name dot11 24ghz slot channel** command.

ap name *ap-name* **dot11 24ghz slot 0 channel** { *channel_number* | **auto** }

Syntax Description

channel_number	Advanced 802.11 channel assignment parameters for Cisco AP. Enter a channel number from 1 - 14.
auto	Enables auto RF.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Usage Guidelines

Example

The following example shows how to configure the channel of an AP.

```
Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 channel auto
```

ap name dot11 24ghz slot cleanair

To enable CleanAir for 802.11b radio hosted on slot 0 for a specific access point, use the **ap name dot11 24ghz slot cleanair** command.

ap name *ap-name* **dot11 24ghz slot 0 cleanair**

Syntax Description

cleanair	Enables 802.11b cleanair management

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.
Cisco IOS XE Cupertino 17.9.1	This command has been deprecated.

Example

The following example shows how to configure the cleanair of an AP.

```
Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 cleanair
```

ap name dot11 24ghz slot dot11n antenna

To configure 802.11n antenna for 2.4-GHz radio hosted on slot 0 for a specific access point, use the **ap name dot11 24ghz slot dot11n antenna** command.

ap name *ap-name* **dot11 24ghz slot 0 dot11n antenna** { **A** | **B** | **C** | **D** }

Syntax Description

dot11n	Configures 802.11n antenna for 2.4-GHz radio hosted on slot 0 for a specific access point.
antenna	Configures the 802.11n - 2.4 GHz antenna selection from antenna ports A, B, C, and D.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Example

The following example shows how to configure the channel width of an AP.

```
Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 dot11n antenna A
```

ap name dot11 24ghz slot dot11ax bss-color

To set the BSS color on the 2.4 GHz, 5 GHz, or dual-band radio, for a specific access point, use the **ap name dot11 24ghz slot dot11ax bss-color** command.

ap name *ap-name* **dot11 24ghz slot 0 dot11ax bss-color** *<1-63>*

Syntax Description

bss-color	Configures 802.11ax-2.4GHz BSS color

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Example

The following example shows how to disable 802.11b radio on Cisco AP.

```
Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 dot11ax bss-color 3
```

ap name dot11 24ghz slot shutdown

To disable 802.11b radio hosted on slot 0 for a specific access point, use the **ap name dot11 24ghz slot shutdown** command.

ap name *ap-name* **dot11 24ghz slot 0 shutdown**

Syntax Description

shutdown	Disables 802.11b radio on Cisco AP

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Example

The following example shows how to disable 802.11b radio on Cisco AP.

```
Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 shutdown
```

ap name dot11 24ghz radio role manual sniffer channel

To enable XOR radio role Sniffer support on AP from controller, use the **ap name dot11 24ghz radio role manual sniffer channel** command.

ap name dot11 24ghz radio role manual sniffer channel *channel-number* **ip** *ip-address*

Syntax Description

channel-number ip *ip-address*	Is the channel number and IP address.

Command Default

None

Command Modes

Global Configuration

Command History

Release	Modification
Cisco IOS XE Cupertino 17.8.1	This command was introduced.

Usage Guidelines

This example shows how to enable XOR radio role Sniffer support on AP from controller:

```
Device# enable
Device# ap name AP687D.B45C.189C dot11 24ghz shutdown
Device# ap name AP687D.B45C.189C dot11 24ghz radio role manual sniffer channel 100 ip
9.4.197.85
Device# ap name AP687D.B45C.189C no dot11 24ghz shutdown
Device# end
```

ap name dot11 5ghz radio role manual sniffer channel

To enable XOR radio role Sniffer support on AP from controller, use the **ap name dot11 5ghz radio role manual sniffer channel** command.

ap name dot11 5ghz radio role manual sniffer channel *channel-number* **ip** *ip-address*

Syntax Description

channel-number ip *ip-address*	Is the channel number and IP address.

Command Default

None

Command Modes

Global Configuration

Command History

Release	Modification
Cisco IOS XE Cupertino 17.8.1	This command was introduced.

Usage Guidelines

This example shows how to enable XOR radio role Sniffer support on AP from controller:

```
Device# enable
Device# ap name AP687D.B45C.189C dot11 5ghz shutdown
Device# ap name AP687D.B45C.189C dot11 5ghz radio role manual sniffer channel 100 ip
9.4.197.85
Device# ap name AP687D.B45C.189C no dot11 5ghz shutdown
Device# end
```

ap name dot11 5ghz slot 1 dual-radio mode

To configure the 802.11a dual radio on the AP, use the **ap name** *ap-name* **dot11 5ghz slot 1 dual-radio mode**

ap name *ap-name* **dot11 5ghz slot 1 dual-radio mode** {**enable** | **disable**}

Syntax Description

dual-radio mode	Configures the 802.11a dual-radio on the AP.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.2.1	This command was introduced.

Example

The following example shows how to configure the 802.11a dual radio on the AP:

```
Device#ap name ap-name dot11 5ghz slot 1 dual-radio mode enable
```

ap name dot11 5ghz slot {1 | 2} urwb dfs

To configure the URWB DFS role on a 5 GHz radio interface, use the **ap name** *ap-name* **dot11 5ghz slot** {**1** | **2**}**urwb dfs** {**auto** | **primary** | **secondary**}

ap name *ap-name* **dot11 5ghz slot** { **1** | **2** } **urwb dfs** { **auto** | **primary** | **secondary** }

Syntax Description

ap-name	Specifies the name of the Cisco AP.
auto	Specifies the URWB DFS role as auto on this radio interface.
primary	Specifies URWB DFS role as primary on this radio interface.
secondary	Specifies URWB DFS role as secondary on this radio interface.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 17.18.1	This command was introduced.

Examples

The following example shows how to configure the URWB DFS role on a 5 GHz radio interface:

```
Device# ap name ap-name 5ghz slot 1 urwb dfs auto
```

ap name dot11 5ghz slot {1 | 2} urwb ptmp base

To enable URWB PTMP base on a 5 GHz radio interface, use the **ap name** *ap-name* **dot11 5ghz slot** {**1** | **2**}**urwb ptmp base**

ap name *ap-name* **dot11 5ghz slot** { **1** | **2** } **urwb ptmp base**

Syntax Description

ap-name	Specifies the name of the Cisco AP.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 17.18.1	This command was introduced.

Examples

The following example shows how to enable URWB PTMP base on a 5 GHz radio interface:

```
Device# ap name ap-name 5ghz slot 1 urwb ptmp base
```

ap name dot11 5ghz slot radio role

To set the manual radio role to either client serving or monitor, use the **ap name** *ap-name* **dot11 5ghz slot** {**1** | **2**} **radio role** command.

ap name *ap-name* **dot11 5ghz slot** { **1** | **2** } **radio role** { **auto** | **manual** { **client-serving** | **monitor** } }

Syntax Description

radio role	Configures the 802.11a radio role, either manual or auto.
manual	Configures either client-serving manual role or monitor manual role.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.2.1	This command was introduced.

Example

The following example shows how to set the manual radio role to either client serving or monitor:

```
Device# ap name ap-name dot11 5ghz slot 2 radio role manual monitor
```

ap name dot11 channel width

To configure the channel width of an AP, use the **ap name dot11 channel width** command.

ap name *ap-name* **dot11** { **24ghz** | **5ghz** | **dual-band** | **rx-dual-band** } **channel width** { **160** | **20** | **40** | **80** | **80+80** }

Syntax Description

ap-name	Name of the Cisco Lightweight Access Point.
160	160 MHz.
20	20 MHz.
40	40 MHz.
80	80 MHz.
80+80	80+80 MHz.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Example

The following example shows how to configure the channel width of an AP.

```
Device# ap name ax1 dot11 5ghz channel width 80+80
```

ap name dot11 dual-band cleanair

To configure CleanAir for a dual band radio, use the **ap name dot11 dual-band cleanair** command.

ap name *ap-name* **dot11 dual-band cleanair**
ap name *ap-name* **no dot11 dual-band cleanair**

Syntax Description

ap-name	Name of the Cisco AP.
cleanair	Specifies the CleanAir feature.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
Cisco IOS XE Cupertino 17.9.1	This command was deprecated.

This example shows how to enable CleanAir for a dual band radio of the access point AP01:

```
Device# ap name AP01 dot11 dual-band cleanair
```

ap name dot11 dual-band shutdown

To disable dual band radio on a Cisco AP, use the **ap name dot11 dual-band shutdown** command.

ap name *ap-name* **dot11 dual-band shutdown**
ap name *ap-name* **no dot11 dual-band shutdown**

Syntax Description

ap-name	Name of the Cisco AP.
shutdown	Disables the dual band radio on the Cisco AP.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

This example shows how to disable dual band radio on the Cisco access point AP01:

```
Device# ap name AP01 dot11 dual-band shutdown
```

ap name dot11 dual-band slot radio role manual client-serving

To switch to client serving mode on a Cisco AP, use the **ap name dot11 dual-band slot radio role manual client-serving** command.

ap name *ap-name* **dot11 dual-band slot** *slot-number* **radio role manual client-serving**

Syntax Description

ap-name	Name of the Cisco AP.
slot-number	Slot downlink radio to which the channel is assigned, valid values are 0 & 2.
radio role	Configures radio role.
manual	Switch to manual radio role selection.
client serving	Switch to client-serving radio role.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
IOS XE 17.15.2	This command was introduced.

This example shows how to switch to client serving mode on the Cisco access point:

```
Device# ap name cisco-ap dot11 dual-band slot 2 radio role manual client-serving
```

ap name dot11 dual-band slot shutdown

To enable or disable dual band radio on a Cisco AP, use the **ap name dot11 dual-band slot shutdown** command.

ap name *ap-name* **dot11 dual-band slot** *slot-number* **shutdown**

Syntax Description

ap-name	Name of the Cisco AP.
slot-number	Radio slot identifier to which the channel is assigned, valid values are 0 & 2.
shutdown	Disables the dual band radio on the Cisco AP.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
IOS XE 17.15.2	This command was introduced.

This example shows how to disable dual band radio on the Cisco access point AP01:

```
Device# ap name AP01 dot11 dual-band slot 2 shutdown
```

ap name dot11 dual-band slot band 6ghz

To enable 6-Ghz on 802.11 dual-band radio on a Cisco AP, use the **ap name dot11 dual-band slot band 6ghz** command.

ap name *ap-name* **dot11 dual-band slot** *slot-number* **band** *6ghz*

Syntax Description

ap-name	Name of the Cisco AP.
slot-number	Radio slot identifier to which the channel is assigned, valid values are 0 & 2.
band	Configures the 802.11 dual-band radio's current band.
6ghz	Switches to 6GHz band.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
IOS XE 17.15.2	This command was introduced.

This example shows how to enable 6-Ghz on 802.11 dual-band radio on the Cisco access point:

```
Device# ap name cisco-ap dot11 dual-band slot 2 band 6ghz
```

ap name dot11 rrm profile

To configure Radio Resource Management (RRM) performance profile settings for a Cisco lightweight access point, use the **ap name dot11 rrm profile** command.

ap name *ap-name* **dot11** {**24ghz** | **5ghz**} **rrm profile** {**clients** *value* | **customize** | **foreign** *value* | **noise** *value* | **throughput** *value* | **utilization** *value*}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
clients	Sets the access point client threshold.
value	Access point client threshold from 1 to 75 clients. **Note** The default client threshold is 12.
customize	Turns on performance profile customization for an access point. **Note** Performance profile customization is off by default.
foreign	Sets the foreign 802.11 transmitter interference threshold.
value	Foreign 802.11 transmitter interference threshold from 0 to 100 percent. **Note** The default is 10 percent.
noise	Sets the 802.11 foreign noise threshold.
value	802.11 foreign noise threshold between –127 and 0 dBm. **Note** The default is —70 dBm.
throughput	Sets the data-rate throughput threshold.
value	802.11 throughput threshold from 1000 to 10000000 bytes per second. **Note** The default is 1,000,000 bytes per second.
utilization	Sets the RF utilization threshold. **Note** The operating system generates a trap when this threshold is exceeded.

value	802.11 RF utilization threshold from 0 to 100 percent. **Note** The default is 80 percent.

Command Default

None

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

This example shows how to set the AP1 clients threshold to 75 clients:

```
Device# ap name AP1 dot11 24ghz rrm profile clients 75
```

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

```
Device# ap name AP1 dot11 5ghz rrm profile customize
```

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

```
Device# ap name AP1 dot11 5ghz rrm profile foreign 0
```

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

```
Device# ap name AP1 dot11 5ghz rrm profile noise 0
```

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

```
Device# ap name AP1 dot11 5ghz rrm profile throughput 10000000
```

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

```
Device# ap name AP1 dot11 5ghz rrm profile utilization 100
```

ap name export support-bundle mode

To export the AP support-bundle from the AP to the controller, use the **ap name** *Cisco-AP-name* **export support-bundle mode**

ap name *Cisco-AP-name* **export support-bundle mode** { **scp** | **tftp** } **target ip-address** { *A.B.C.D* | *X:X:X:X::X* } **path** *file-path*

Syntax Description

scp	Transfers the support-bundle through the SCP mode.
tftp	Transfers the support-bundle through the TFTP mode.
target	Indicates the target details for file transfer using TFTP.
ip-address	Indicates the target IP address, either IPv4 or IPv6, for the file transfer using SCP or TFTP.
A.B.C.D	Indicates the target IPv4 address.
X:X:X:X::X	Indicates the target IPv6 address.
path	Indicates the target file path.
file-path	Indicates the file path.

Command Default

None

Command Modes

Privileged EXEC mode

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.3.1	This command was introduced.

Example

This example shows how to export the AP support-bundle from the AP to the controller:

```
Device> ap name Cisco-AP-name export support-bundle mode scp target ip-address 10.1.1.1
path file-path
```

ap name floor

To configure the floor ID for an AP, use the **ap name** *cisco-ap-name* **floor** *floor-id* command.

ap name *cisco-ap-name* **floor** *floor-id*

Syntax Description

cisco-ap-name	Specifies a Cisc
floor-id	Specifies the floor ID of the AP. The floor ID values are between -2147483648 and 2147483647.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Dublin 17.12.1	This command was introduced.

Example

This example shows how to configure the floor ID for an AP:

```
Device# ap name cisco-ap-name floor 20
```

ap name geolocation coordinate

To configure the longitude and latitude of a Cisco AP, use the **ap name geolocation coordinate** command.

ap name *ap-name* **geolocation coordinate** *longitude latitude*

Syntax Description

ap-name	Name of the Cisco AP.
longitude	Configures the longitude of the AP. The valid range for longitude is between -180 and 180 degrees.
latitude	Configures the latitude of the AP. The valid range for latitude is between -90 and 90 degrees.

Command Default

None

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Dublin 17.12.1	This command was introduced.

Examples

The following example shows how to configure the longitude and latitude of a Cisco AP:

```
Device# ap name geolocation coordinate longitude 180
```

ap name geolocation gnss antenna external cable-length

To configure the external cable length of a Global Navigation Satellite System (GNSS), use the **ap name geolocation gnss antenna external cable-length** command.

ap name *ap-name* **geolocation gnss antenna external cable-length** *cable-length*

Syntax Description

ap-name	Name of the Cisco AP.
cable-length	Configures the GNSS antenna external cable length of a Cisco AP in meters. The valid values range from 1 to 100, with a default value of 10m.

Command Default

None

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Dublin 17.12.2	This command was introduced.

Examples

The following example shows how to configure the external cable length of a GNSS:

```
Device# ap name geolocation gnss antenna external cable-length 45
```

ap name geolocation height uncertainty

To configure the uncertainty geolocation height of a Cisco AP, use the **ap name geolocation height uncertainty** command.

ap name *ap-name* **geolocation height** *height* **uncertainty** *uncertainty*

Syntax Description

ap-name	Name of the Cisco AP.
height	Specifies the Above Ground Level (AGL) height in meters. The valid values range from -100 to 1000.
uncertainty	Specifies the uncertainty height of an AP in meters. The valid values range from 1 to 100.

Command Default

None

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Dublin 17.12.1	This command was introduced.

Examples

The following example shows how to configure the uncertainity geolocation height of a Cisco AP:

ap name hyperlocation

To configure hyperlocation and related parameters for an access point (AP), use the **ap name hyperlocation** command. To disable hyperlocation and related parameters, use the **no** form of this command.

ap name *ap-name* **hyperlocation ble-beacon** *beacon-id* { **major** *major-value* | **minor** *minor-value* | **txpwr** *att-value* }

Syntax Description

ap-name	Access point name.
ble-beacon	Configures BLE beacon parameters.
beacon-id	BLE beacon ID.
major	Configures BLE beacon major parameter.
major-value	BLE beacon major value. The range is from 0 to 65535. The default is 0.
minor	Configures BLE beacon minor parameter.
minor-value	BLE beacon minor value. The range is from 0 to 65535. The default is 0.
txpwr	Configures BLE beacon attenuation level.
att-value	BLE beacon attenuation value, in dBm. The range is from 0 to 52. The default is 0.

Command Default

BLE beacon details are not configured.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Example

This example shows how to configure hyperlocation and related parameters for an AP:

```
Device# ap name test-ap hyperlocation ble-beacon 3 txpwr 50
```

ap name image

To configure an image on a specific access point, use the **ap name image** command.

ap name *ap-name* **image** {**predownload** | **swap**}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
predownload	Instructs the access point to start the image predownload.
swap	Instructs the access point to swap the image.

Command Default

None

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

This example shows how to predownload an image to an access point:

```
Device# ap name AP2 image predownload
```

This example shows how to swap an access point's primary and secondary images:

```
Device# ap name AP2 image swap
```

ap name icap subscription client anomaly-detection report-individual enable aggregate

To configure anomaly detection for client subscriptions and to enable individual report aggregation, use the **ap name icap subscription client anomaly-detection report-individual enable aggregate** command.

ap name *ap name* **icap subscription client anomaly-detection report-individual enable aggregate**

Syntax Description

ap name	Name of the Cisco access point.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Dublin 17.12.1	This command was introduced.

Examples

The following example shows how to configure anomaly detection for client subscriptions and to enable individual report aggregation:

```
Device# ap name cisco-AP icap subscription client anomaly-detection report-individual enable
 aggregate
```

ap name icap subscription client anomaly-detection report-individual per-client throttle

To configure individual reports per client every five minutes on an AP, use the **ap name icap subscription client anomaly-detection report-individual per-client throttle** command.

ap name *ap name* **icap subscription client anomaly-detection report-individual per-client throttle** *throttle-value*

Syntax Description

ap name	Name of the Cisco access point.
throttle-value	Number of event reports per client. Valid value ranges from 0 to 50. If the value is 0, there is no throttle.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Dublin 17.12.1	This command was introduced.

Examples

The following examples shows how to configure individual reports per client every five minutes on an AP:

```
Device# ap name cisco-AP icap subscription client anomaly-detection report-individual
per-client throttle 10
```

ap name icap subscription client anomaly-detection report-individual per-type throttle

To configure individual reports per type on an AP, use the **ap name icap subscription client anomaly-detection report-individual per-type throttle** command.

ap name *ap name* **icap subscription client anomaly-detection report-individual per-type throttle** *throttle*

Syntax Description

ap name	Name of the Cisco access point.
throttle-value	Number of event reports per client. Valid values range from 0 to 100. If the value is 0, there is no throttle.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Dublin 17.12.1	This command was introduced.

Examples

The following example shows how to configure individual reports per type on an AP:

```
Device# ap name cisco-AP icap subscription client anomaly-detection report-individual
per-type throttle 50
```

ap name indoor

To enable the access point in the indoor mode, use the **ap name** *ap name* **indoor** command.

ap name *ap_name* **indoor**

Syntax Description

ap name	AP Name
indoor	Enables the access point in the indoor mode.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Examples

The following example shows how to enable the access point in the indoor mode:

```
Device# ap name test indoor
```

ap name iot-radio firmware overwrite

To set the IoT radio firmware to default, use the **ap name** *ap-name* **iot-radio firmware overwrite** command.

ap name *ap-name* **iot-radio firmware overwrite**

Syntax Description

ap-name	Specifies the name of the Cisco AP.

Command Default

None

Command Modes

Privileged EXEC mode

Command History

Release	Modification
Cisco IOS XE Cupertino 17.7.1	This command was introduced.

Example

This example shows how to set the IoT radio firmware to default:

```
Device# ap name Cisco-ap iot-radio firmware overwrite
```

ap name ipsla

To configure ipsla on the AP, use the **ap name** *ap name* **ipsla** command.

ap name *ap_name* **ipsla**

Syntax Description

ap name	AP Name
ipsla	Enables the ipsla on the access point.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Examples

The following example shows how to configure ipsla on the access point:

```
Device# ap name test ipsla
```

ap name keepalive

To enable the keepalive option on the AP, use the **ap name** *ap name* **keepalive** command.

ap name *ap_name* **keepalive**

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 17.03.1	This command was introduced.

Examples

The following example shows how to enable the keepalive option on the AP:

```
Device# ap name test keepalive
```

ap name lan

To configure LAN port configurations for APs, use the **ap name lan** command. To remove LAN port configurations for APs, use the**ap name no lan** command.

ap name *ap-name* **[no]lan port-id** *port-id* {**shutdown** | **vlan-access**}

Syntax Description

no	Removes LAN port configurations.
port-id	Configures the port.
port-id	The ID of the port. The range is 1-4
shotdown	Disables the Port.
vlan-access	Enables VLAN access to Port.

Command Default

None

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

This example shows how to enable VLAN access to port:

```
Device# ap name AP1 lan port-id 1 vlan-access
```

ap name led

To enable the LED state for an access point, use the **ap name led** command. To disable the LED state for an access point, use the **no** form of this command.

ap name *ap-name* **led**
no ap name *ap-name* [**led**] **led**

Syntax Description

ap-name	Name of the Cisco lightweight access point.
led	Enables the access point's LED state.

Command Default

None

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

This example shows how to enable the LED state for an access point:

```
Device# ap name AP2 led
```

This example shows how to disable the LED state for an access point:

```
Device# ap name AP2 no led
```

ap name led-brightness-level

To configure the LED brightness level on the AP, use the **ap name** *ap name* **led-brightness-level** command.

ap name *ap_name* **led-brightness-level {1–8}**

Syntax Description

ap name	AP Name
led brightness level	Configures the led brightness level. **Note** Valid led brightness level is from 1 to 8.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Examples

The following example shows the LED brightness level on the access point:

```
Device# ap name cisco-ap led-brightness-level2
```

ap name location

To modify the descriptive location of a Cisco lightweight access point, use the **ap name location** command.

ap name *ap-name* **location** *location*

Syntax Description

ap-name	Name of the Cisco lightweight access point.
location	Location name of the access point (enclosed by double quotation marks).

Command Default

None

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

The Cisco lightweight access point must be disabled before changing this parameter.

This example shows how to configure the descriptive location for access point AP1:

```
Device# ap name AP1 location Building1
```

ap name mesh backhaul rate dot11abg

To set the mesh backhaul dot11abg rate, use the **ap name** *ap-name* **mesh backhaul rate dot11abg** command.

ap name *ap-name* **mesh backhaul rate dot11abg** { **RATE_11M** | **RATE_12M** | **RATE_18M** | **RATE_1M** | **RATE_24M** | **RATE_2M** | **RATE_36M** | **RATE_48M** | **RATE_54M** | **RATE_5DOT5M** | **RATE_6M** | **RATE_9M** }

Syntax Description

RATE_11M | **RATE_12M** | **RATE_18M** | **RATE_1M** | **RATE_24M** | **RATE_2M** | **RATE_36M** | **RATE_48M** | **RATE_54M** | **RATE_5DOT5M** | **RATE_6M** | **RATE_9M**	Sets the mesh backhaul rates.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.6.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows you how to configure the AP mesh backhaul dot11abg rate:

```
Device# ap name cisco-ap mesh backhaul rate dot11abg RATE_11M
```

ap name mdsn-ap

To configure mdsn-ap on the AP, use the **ap name** *ap name* **mdsn-ap** command.

ap name *ap_name* **mdsn-ap {disable | enable | vlan}** *add delete*

Syntax Description

ap name	AP Name
disable	Disables the mDNS access point.
enable	Enables the mDNS access point.
vlan	Adds or deletes the VLAN from mDNS access point.
add	Adds vlan to mDNS AP.
add	Deletes vlan from the mDNS AP.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Examples

The following example shows how to enable mdns on the AP:

```
Device# Device# ap name test mdns enable
```

ap name mesh backhaul rate dot11ac

To set the mesh backhaul dot11ac rate, use the **ap name** *ap-name* **mesh backhaul rate dot11ac** command.

ap name *ap-name* **mesh backhaul rate dot11ac mcs** *0-9* **ss** *1-4*

Syntax Description

mcs *0-9*	Sets the mesh backhaul 11ac MCS rate.
0-9	Indicates the mesh backhaul rate 11ac mcs index .
ss	Sets the mesh backhaul 11ac spatial stream.
1-4	Indicates the mesh backhaul 11ac spatial stream value.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.6.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows you how to configure the AP mesh backhaul dot11ac rate:

```
Device# ap name cisco-ap mesh backhaul rate dot11ac mcs 5 ss 3
```

ap name name mesh backhaul rate dot11ax

To set the mesh backhaul dot11ax rate, use the **ap name** *ap-name* **mesh backhaul rate dot11ax** command.

ap name *ap-name* **mesh backhaul rate dot11ax mcs** *0-11* **ss** *1-8*

Syntax Description

mcs	Sets the mesh backhaul 11ax MCS rate.
0-11	Indicates the mesh backhaul 11ax MCS index.
ss	Sets the mesh backhaul 11ax spatial stream.
1-8	Indicates the mesh backhaul 11ax spatial stream value. Range 1-4 indicates the range for 2.4-Ghz, and range 1 - 8 indicates the range for 5-Ghz backhaul.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.6.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows you how to configure the AP mesh backhaul dot11ax rate:

```
Device# ap name cisco-ap mesh backhaul rate dot11ax mcs 6 ss 5
```

ap name name new-ap-name

To configure the new Cisco AP name, use the **ap name** *ap name* **name** *new-ap-name* command.

ap name *ap_name* **name** *new-ap-name*

Syntax Description

ap name	AP Name
name	Specifies the new Cisco AP name.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Examples

The following example shows how to configure the new Cisco AP:

```
Device# ap name test name test2
```

ap name no

To negate a command or set its defaults on the AP, use the **no** command.

ap name *ap_name* **no**

Syntax Description

ap name	AP Name
no	Negate a command or set its defaults.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Examples

The following example shows how to negate a command or set its defaults on the AP:

```
Device# ap name test no
```

ap name mesh backhaul rate

To configure the AP mesh backhaul rate, use the **ap name** *ap-name* **mesh backhaul rate** command.

ap name *ap-name* **mesh backhaul rate** { **auto** | **dot11abg** | **dot11ac** | **dot11ax** | **dot11n** }

Syntax Description

auto	Configures the mesh backhaul rate as auto.
dot11abg	Configures the mesh backhaul dot11abg rate.
dot11ac	Configures the mesh backhaul dot11ac rate.
dot11ax	Configures the mesh backhaul dot11ax rate.
dot11n	Configures the mesh backhaul dot11n rate.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.6.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows you how to configure the AP mesh backhaul rate as auto:

```
Device# ap name cisco-ap mesh backhaul rate auto
```

ap name mesh backhaul rate dot11n

To set the mesh backhaul dot11n rate, use the **ap name** *ap-name* **mesh backhaul rate dot11n** command.

ap name *ap-name* **mesh backhaul rate dot11n mcs** *0-31*

Syntax Description

mcs *0-31*	Sets the mesh backhaul 11n MCS rate.
0-31	Indicates the mesh backhaul rate dot11n mcs index.s

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.6.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows you how to configure the AP mesh backhaul dot11n rate:

```
Device# ap name cisco-ap mesh backhaul rate dot11n mcs 20
```

ap name mesh block-child

To set mesh block-child state for a mesh AP, use the **ap name mesh block-child** command.

ap name *ap-name* **mesh block-child**

Syntax Description

ap-name	Name of the mesh AP.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure the mesh block-child state for a mesh AP:

```
Device# ap name mymeshap mesh block-child
```

ap name mesh daisy-chaining

To configure daisy-chain mode for a mesh AP, use the **ap name** *ap-name* **mesh daisy-chaining** command.

ap name *ap-name* **mesh daisy-chaining** [**strict-rap**]

Syntax Description

ap-name	Name of the mesh AP.
strict-rap	Configures to allow only the Ethernet interface as mesh uplink.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure daisy-chaining mode for a mesh AP:

```
Device# ap name mymeshap mesh daisy-chaining
```

ap name mesh ethernet mode access

To configure the mode of Ethernet interface as access for a mesh AP, use the **ap name** *ap-name* **mesh ethernet** *port-no* **mode access** command.

ap name *ap-name* **mesh ethernet** *port-no* **mode access** *vlan-id*

Syntax Description

ap-name	Name of the mesh AP.
port-no	Port number of the AP. Valid options are 1, 2, 3, and 4.
vlan-id	VLAN ID. Valid range is from 0 to 4095.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure the mode of Ethernet interface as access for a mesh AP:

```
Device# ap name mymeshap mesh ethernet 0 mode access 10
```

ap name mesh ethernet mode trunk

To configure the mode of Ethernet interface as trunk for a mesh AP, use the **ap name** *ap-name* **mesh ethernet** *port-no* **mode trunk** command.

ap name *ap-name* **mesh ethernet** *port-no* **mode trunk vlan** {**allowed** | **native**} *vlan-id*

Syntax Description

ap-name	Name of the mesh AP.
port-no	Port number of the AP. Valid options are 1, 2, 3, and 4.
allowed	Configures allowed VLANs for the trunk port.
native	Configures native VLAN for the trunk port.
vlan-id	VLAN ID. Valid range for allowed VLANs is from 0 to 4095. Valid range for native VLANs is 1 to 4095.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure the mode of Ethernet interface as trunk for a mesh AP and also configure allowed VLANs for the trunk port:

```
Device# ap name mymeshap mesh ethernet 0 mode trunk vlan allowed 10
```

ap name mesh linktest

To perform a link test with a mesh AP, use the **ap name** *ap-name***mesh linktest** command.

ap name *ap-name* **mesh linktest** *dest-ap-mac data-rate pkts-per-sec pkt-size test-duration*

Syntax Description

ap-name	Name of the mesh AP.
dest-ap-mac	MAC address of the destination mesh AP.
data-rate	Data rate in Mbps (1, 2, 5.5, 6, 9, 11, 12, 24, 36, 48, 53, m0-m15)
pkts-per-sec	Packets to be sent per second. Valid range is from 1 to 25000.
pkt-size	Packet size. Valid range is from 1 to 1500.
test-duration	Test duration. Valid range is from 10 to 300 seconds.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure a link test for a mesh AP:

```
Device# ap name mymeshap mesh linktest 00c0.00a0.03fa.0000.0000.0000
 9 100 10 180
```

ap name mesh parent preferred

To configure preferred parent for a mesh AP, use the **ap name mesh parent preferred** command.

ap name *ap-name* **mesh parent preferred** *mac-address*

Syntax Description

ap-name	Name of the mesh AP.
mac-address	Radio MAC address of the parent AP.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to preferred parent for a mesh AP:

```
Device # ap name mymeshap mesh parent preferred dc:5f:be:f5:fd:84
```

ap name mesh security psk provisioning delete

To delete PSK-provisioned key from a mesh AP, use the **ap name mesh security psk provisioning delete** command.

ap name *ap-name* **mesh security psk provisioning delete**

Syntax Description

ap-name	Name of the mesh AP.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to delete PSK-provisioned key from a mesh AP:

```
Device# ap name mymeshap mesh security psk provisioning delete
```

ap name mesh vlan-trunking native

To configure native VLAN for mesh AP, use the **ap name mesh vlan-trunking native** command.

ap name *name-of-rap* **vlan-trunking native** *vlan-id*

Syntax Description

name-of-rap	Name of the root access point.
vlan-id	VLAN ID.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Example

The following example shows how to configure native VLAN for mesh AP:

```
Device # ap name mesh vlan-trunking native 12
```

ap name mode

To change a Cisco device communication option for an individual Cisco lightweight access point, use the **ap name mode** command.

ap name *ap-name* **mode** {**local submode** {**none** | **wips**} | **monitor submode** {**none** | **wips**} | **rogue** | **se-connect** | **sniffer**}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
local	Converts from an indoor mesh access point (MAP or RAP) to a nonmesh lightweight access point (local mode).
submode	Specifies wIPS submode on an access point.
none	Disables the wIPS on an access point.
monitor	Specifies monitor mode settings.
wips	Enables the wIPS submode on an access point.
rogue	Enables wired rogue detector mode on an access point.
se-connect	Enables spectrum expert mode on an access point.
sniffer	Enables wireless sniffer mode on an access point.

Command Default

Local

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

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.

This example shows how to set the device to communicate with access point AP01 in local mode:

```
Device# ap name AP01 mode local submode none
```

This example shows how to set the device to communicate with access point AP01 in a wired rogue access point detector mode:

```
Device# ap name AP01 mode rogue
```

This example shows how to set the device to communicate with access point AP02 in wireless sniffer mode:

```
Device# ap name AP02 mode sniffer
```

ap name mode bridge

To configure Bridge mode for an AP, use the **ap name** *ap-name* **mode bridge** command.

ap name *ap-name* **mode bridge**

Syntax Description

ap-name	Name of the AP.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure a Bridge mode for an AP:

```
Device# ap name my-ap mode bridge
```

ap name monitor-mode

To configure Cisco lightweight access point channel optimization, use the **ap name monitor-mode** command.

ap name *ap-name* **monitor-mode** {**no-optimization** | **tracking-opt** | **wips-optimized**}

Syntax Description

ap-name	Name of the Cisco lightweight 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.

Command Default

None

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

This example shows how to configure a Cisco wireless intrusion prevention system (wIPS) monitor mode on access point AP01:

```
Device# ap name AP01 monitor-mode wips
```

ap name monitor-mode dot11b

To configures 802.11b scanning channels for a monitor-mode access point, use the **ap name monitor-mode dot11b** command.

ap name *ap-name* **monitor-mode dot11b fast-channel** *channel1* [*channel2*] [*channel3*] [*channel4*]

Syntax Description

ap-name	Name of the access point.
fast-channel	Specifies the 2.4 GHz band scanning channel (or channels) for a monitor-mode access point.
channel1	Scanning channel1.
channel2	(Optional) Scanning channel2.
channel3	(Optional) Scanning channel3.
channel4	(Optional) Scanning channel4.

Command Default

None

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

This example shows how to configure an access point in tracking optimized mode to listen to channels 1, 6, and 11:

```
Device# ap name AP01 monitor-mode dot11b fast-channel 1 6 11
```

ap name management-mode meraki

To change AP Management Mode to Meraki, use the **ap name management-mode meraki** command.

ap name management-mode meraki

Syntax Description

force	Skips the validations at the controller and attempts Meraki Management Mode change at the AP.
noprompt	Skips the user prompt for attempting AP Management Mode change.
cisco-ap-name	Specifies the name of the Cisco AP for Management Mode change.

Command Default

None

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Cupertino 17.9.1	This command was modified.

Example

This example shows how to change AP Management Mode to Meraki:

```
Device# ap name Cisco-AP-name management-mode meraki
Device# ap name Cisco-AP-name management-mode meraki force
Device# ap name Cisco-AP-name management-mode meraki noprompt
Device# ap name Cisco-AP-name management-mode meraki force noprompt
```

ap name name

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

ap name *ap-name* **name** *new-name*

Syntax Description

ap-name	Current Cisco lightweight access point name.
new-name	Desired Cisco lightweight access point name.

Command Default

None

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

This example shows how to modify the name of access point AP1 to AP2:

```
Device# ap name AP1 name AP2
```

ap name network-diagnostics

To trigger network diagnostics on an OfficeExtend AP, use the **ap name network-diagnostics** command.

ap name *ap-name* **network-diagnostics**

Syntax Description

ap-name	Name of the access point.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.5.1	This command was introduced.

Example

This following example shows how to trigger network diagnostics on an OfficeExtend AP.

```
Device# ap name ap18 network-diagnostic
```

ap name priority

To configure the priority of an access point, use the **ap name priority** command.

ap name *ap-name* **priority** *priority-value*

Syntax Description

priority-value	Priority value for the AP. Valid range is 1 to 4.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure the priority for an access point:

```
Device# ap name my-ap priority 1
```

ap name remote

To initiate AP remote commands, use the **ap name** *ap-name* **remote** command.

ap name *ap-name* **remote** { **command** *command-name* | **disable** | **enable** }

Syntax Description

remote command *command-name*	Initiates the AP remote command.
disable	Initiates the AP remote disable command.
enable	Initiates the AP remote enable command.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.3.1	This command was introduced.

Usage Guidelines

None

Example

This example shows how to initiate AP remote commands:

```
Device# terminal monitor
Device# ap name ap-name remote enable
Device# ap name ap-name remote command 'show client sum'
.
.
.
Device# ap name ap-name remote disable
```

Note To view the output in real-time, use the **terminal monitor** command. To view the output in the controller log, use the **show logging** command.

ap name reset

To reset a specific Cisco lightweight access point, use the **ap name reset** command.

ap name *ap-name* **reset**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

This example shows how to reset a Cisco lightweight access point named AP2:

```
Device# ap name AP2 reset
```

ap name reset-button

To configure the Reset button for an access point, use the **ap name reset-button** command.

ap name *ap-name* **reset-button**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

This example shows how to enable the Reset button for access point AP03:

```
Device# ap name AP03 reset-button
```

ap name role

To configure the role of operation for an AP, use the **ap name role** command.

ap name *ap-name* **role** {**mesh-ap** | **root-ap**}

Syntax Description

ap-name	Name of the AP.
mesh-ap	Configures mesh AP role for the AP.
root-ap	Configures root AP role for the AP.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure the role of operation as mesh AP for an AP:

```
Device# ap name mymeshap role mesh-ap
```

ap name sensor environment

To disable the sensor admin state of the AP, use the **ap name** *cisco-ap-name* **sensor environment** command. Use the **no** form of this command to enable the sensor admin state of the AP.

ap name *cisco-ap-name* **sensor environment** { **air-quality** | **temperature** } **shutdown**

ap name *cisco-ap-name* **no sensor environment** { **air-quality** | **temperature** } **shutdown**

Syntax Description

air-quality	Specifies the air quality sensor.
temperature	Specifies the temperature and humidity sensor.
shutdown	Shuts down the specified sensor.

Command Default

None

Command Modes

Privileged EXEC #

Command History

Release	Modification
Cisco IOS XE Cupertino 17.8.1	This command was introduced.

Example

The following example shows you how to disable the sensor admin state of the AP:

```
Device# enable
Device# ap name cisco-ap-name sensor environment temperature shutdown
```

ap name slot

To configure various slot parameters, use the **ap name slot** command. To disable a slot on a Cisco lightweight access point, use the **no** form of this command.

ap name *ap-name* **slot** *slot-number* {**channel** {**global** | **number** *channel-number* | **width** *channel-width*} | **rtsthreshold** *value* | **shutdown** | **txpower** {**global***channel-level*}}
ap name *ap-name* **no slot** {**0** | **1** | **2** | **3**} **shutdown**

Syntax Description

ap-name	Name of the Cisco access point.
slot-number	Slot downlink radio to which the channel is assigned. You can specify the following slot numbers: • **0**—Enables slot number 0 on a Cisco lightweight access point. • **1**—Enables slot number 1 on a Cisco lightweight access point. • **2**—Enables slot number 2 on a Cisco lightweight access point. • **3**—Enables slot number 3 on a Cisco lightweight access point.
channel	Specifies the channel for the slot.
global	Specifies channel global properties for the slot.
number	Specifies the channel number for the slot.
channel-number	Channel number from 1 to 169.
width	Specifies the channel width for the slot.
channel-width	Channel width from 20 to 40.
rtsthreshold	Specifies the RTS/CTS threshold for an access point.
value	RTS/CTS threshold value from 0 to 65535.
shutdown	Shuts down the slot.
txpower	Specifies Tx power for the slot.
global	Specifies auto-RF for the slot.
channel-level	Transmit power level for the slot from 1 to 7.

Command Default

None

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

This example shows how to enable slot 3 for the access point abc:

```
Device# ap name abc slot 3
```

This example shows how to configure RTS for the access point abc:

```
Device# ap name abc slot 3 rtsthreshold 54
```

ap name static-ip

To configure lightweight access point static IP settings, use the **ap name static-ip** command. To disable the Cisco lightweight access point static IP address, use the **no** form of this command.

ap name *ap-name* **static-ip** {**domain** *domain-name* | **ip-address** *ip-address* **netmask** *netmask* **gateway** *gateway* | **nameserver** *ip-address*}
ap name *ap-name* **no static-ip**

Syntax Description

ap-name	Name of the access point.
domain	Specifies the Cisco access point domain name.
domain-name	Domain to which a specific access point belongs.
ip-address	Specifies the Cisco access point static IP address.
ip-address	Cisco access point static IP address.
netmask	Specifies the Cisco access point static IP netmask.
netmask	Cisco access point static IP netmask.
gateway	Specifies the Cisco access point gateway.
gateway	IP address of the Cisco access point gateway.
nameserver	Specifies a DNS server so that a specific access point can discover the device using DNS resolution.
ip-address	IP address of the DNS server.

Command Default

None

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

An access point cannot discover the device 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.

This example shows how to configure an access point static IP address:

```
Device# ap name AP2 static-ip ip-address 192.0.2.54 netmask 255.255.255.0 gateway 192.0.2.1
```

ap name shutdown

To disable a Cisco lightweight access point, use the **ap name shutdown** command. To enable a Cisco lightweight access point, use the **no** form of this command.

ap name *ap-name* **shutdown**
ap name *ap-name* **no shutdown**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

This example how to disable a specific Cisco lightweight access point:

```
Device# ap name AP2 shutdown
```

ap name sniff

To enable sniffing on an access point, use the **ap name sniff** command. To disable sniffing on an access point, use the **no** form of this command.

ap name *ap-name* **sniff** { **dot116Ghz** | **dot11a** | **dot11b** }
ap name *ap-name* **no sniff** { **dot11a** | **dot11b** | **dot116Ghz** }

Syntax Description

ap-name	Name of the Cisco lightweight access point.
dot116Ghz	Specifies the 6-GHz band.
dot11a	Specifies the 2.4-GHz band.
dot11b	Specifies the 5-GHz band.
channel	Valid channel to be sniffed. For the 5 GHz band, the range is 36 to 165. For the 2.4 GHz band, the range is 1 to 14. For dot11 6Ghz, the range is between 1 and 233.
server-ip-address	IP address of the remote machine running Omnipeek, Airopeek, AirMagnet, or Wireshark software.

Command Default

Channel 36

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
Cisco IOS XE Cupertino 17.7.1	This command was modified to add 6-GHz.

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 about 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 that are sent by the access point.

This example shows how to enable the sniffing on the 5 GHz band for an access point on the primary wireless LAN controller:

```
Device# ap name AP2 sniff dot11a 36 192.0.2.54
```

ap name tftp-downgrade

To configure the settings used for downgrading a lightweight access point to an autonomous access point, use the **ap name tftp-downgrade** command.

ap name *ap-name* **tftp-downgrade** *tftp-server-ip* *filename*

Syntax Description

ap-name	Name of the Cisco lightweight access point.
tftp-server-ip	IP address of the TFTP server.
filename	Filename of the access point image file on the TFTP server.

Command Default

None

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

This example shows how to configure the settings for downgrading access point AP1:

```
Device# ap name Ap01 tftp-downgrade 172.21.12.45 ap3g1-k9w7-tar.124-25d.JA.tar
```

ap name urwb mode coordinator radio-off

To configure an AP as a URWB coordinator and to configure the radio-off mode, use the **ap name** *ap-name* **urwb mode coordinator radio-off** {**fixed** | **mobility**}

ap name *ap-name* **urwb mode coordinator radio-off** { **fixed** | **mobility** }

Syntax Description

ap-name	Specifies the name of the Cisco AP.
fixed	Configures the coordinator radio-off fixed mode.
mobility	Configures the coordinator radio-off fixed mode.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 17.18.1	This command was introduced.

Examples

The following example shows how to configure an AP as a URWB coordinator and to configure the radio-off mode:

```
Device# ap name ap-name urwb mode coordinator radio-off fixed
```

ap name usb-module

To enable the USB port on the access point (AP), use the **ap name** *ap-name* **usb-module**. To disable the feature, use the **no** form of this command.

ap name *ap-name* **usb-module**

no ap name *ap-name* **usb-module**

Syntax Description

usb-module	Enables the USB port on the AP.

Command Default

None

Command Modes

Privileged EXEC mode

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.4.1	This command was introduced.

Usage Guidelines

None

Example

This example shows you how to enable the USB port on the AP:

```
Device# ap name ap-name usb-module
```

ap name vlan-tag

To configure VLAN tagging for a nonbridge AP, use the **ap name vlan-tag** command.

ap name *ap-name* **vlan-tag** *vlan-id*

Syntax Description

ap-name	Access point name.
vlan-id	VLAN identifier.

Command Default

VLAN tagging is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Example

The following example shows how to configure VLAN tagging for a nonbridge AP:

```
Device# ap name AP1 vlan-tag 12
```

ap name write tag-config

To write the existing configuration to an AP, use the **ap name write tag-config** command in privileged EXEC mode

ap name *ap-name***write tag-config**

Syntax Description

ap-name	Name of the access point.

Command Default

None

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Usage Guidelines

Use this command to write the existing configuration to an AP.

Example

This example shows how to write the existing configuration to an AP:

```
Device# ap name AP40CE.2485.D594 write tag-config
```

ap name-regex

To configure filter based on AP name regular expression to match with, use the **ap name-regex** command.

ap name-regex *regular-expression*

Syntax Description

regular-expression	Enter the filter string.

Command Default None

Command Modes Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure filter based on AP name regular expression match with:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap filter name filter--name
Device(config-ap-filter)# ap name-regex regular-expression-string
```

ap neighborhood calendar-profile

To select the AP neighborhood calendar profile, use the **ap neighborhood calendar-profile** command.

ap neighborhood calendar-profile *calendar-profile-name*

Syntax Description

calendar-profile-name	Calendar profile name.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Dublin 17.12.1	This command was introduced.

Usage Guidelines

Create a calendar profile before adding the profile under an AP neighborhood configuration.

Example

The following example shows how to select the AP neighborhood calendar profile:

```
Device# configure terminal
Device(config)# ap neighborhood calendar-profile ap-calendar-profile
```

ap neighborhood load-balance

To apply, clear, or start RRM-based AP load balancing, use the **ap neighborhood load-balance** command.

ap neighborhood load-balance { **apply** | **clear** | **start** }

Syntax Description

apply	Performs on-demand RRM-based AP load-balancing.
clear	Clears AP neighborhood load-balancing actions and resource allocation output.
start	Starts AP neighborhood load-balance actions and allocates resources.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Dublin 17.12.1	This command was introduced.

Usage Guidelines

The **start** keyword clears old iteration data, if any, from database and starts the algorithm run. This command is similar to a calendar profile start timer expiry event.

Examples

The following example shows how to start AP neighborhood load-balance actions:

```
Device# ap neighborhood load-balance start
```

ap packet-capture

To start or stop the AP packet capture process, use the **ap packet-capture** command.

ap packet-capture {**start** | **stop**} *client-mac-address* {**auto** | **static** *ap-name*}

Syntax Description

client-mac-address	Client MAC address.
ap-name	AP name.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

When using the **stop** option with **ap packet capture** command, use the keyword **all** to stop the packet capture.

Example

The following example shows how to start the AP packet capture process:

```
Device# ap packet-capture start 3c08.f672.1ad9 static AP_2029
```

The following example shows how to stop the AP packet capture process fully:

```
Device# ap packet-capture stop 3c08.f672.1ad9 all
```

ap packet-capture profile

To configure the AP packet capture profile, use the **ap packet-capture profile**command.

ap packet-capture profile *profile-name*

Syntax Description

profile-name	AP packet capture profile name.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Example

The following example shows how to configure the AP packet capture profile:

```
Device# ap packet-capture profile test1
```

ap packet-capture start

To enables packet capture for the specified client on a set of nearby access points, use the **ap packet-capture start** command.

ap packet-capture start *client-mac-addr* {**auto** | **static** *ap-name*}

Syntax Description

client-mac-addr	MAC address of the client whose packet capture has to be done.
auto	Starts packet capture in the nearby APs.
static *ap-name*	Name of the AP in which the packet capture has to be done.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to enable packet capture for a client on a set of nearby access points:

```
Device# ap packet-capture start 0011.0011.0011 auto
```

ap profile

To configure access point profile, use the **ap profile** command.

ap profile *profile-name*

Syntax Description

profile-name	Enter the name of the AP profile.

Command Default

By default, the AP profile name is default-ap-profile.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure AP profile name:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap profile my-ap-profile
```

ap regulatory activation apply

To apply the regulatory domain configuration, run the **ap regulatory activation apply** command.

ap regulatory activation apply

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Cisco IOS XE 17.15.1	This command was introduced.

Examples

The following example shows you how to apply the regulatory domain configuration:

```
Device# ap regulatory activation apply
```

ap regulatory activation clear

To clear the AP MAC to country mapping records, run the **ap regulatory activation clear** command.

ap regulatory activation clear { **all** | **mac** }

Syntax Description

all	Clears all the AP MAC to country mapping records.
mac	Clears specific AP MAC addresses that need to be removed from the database.
mac-address	Specifies the AP MAC address that needs to be removed.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Cisco IOS XE 17.15.1	This command was introduced.

Examples

The following example shows you how to clear the AP MAC to country mapping records:

```
Device# ap regulatory activation clear all
```

ap regulatory activation file

To configure the AP MAC country mapping details from a static regulatory domain file, run the **ap regulatory activation file** command.

ap regulatory activation file *filename*

Syntax Description

filename	Specifies the name of the regulatory domain activation file.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Cisco IOS XE 17.15.1	This command was introduced.

Examples

The following example shows you how to configure the AP MAC country mapping details from a static regulatory domain file:

```
Device# ap regulatory activation file reg-ap-file.json
```

ap remote-lan profile-name

To configure remote LAN profile, use the **ap remote-lan profile-name** command.

ap remote-lan profile-name *remote-lan-profile-name rlan-id*

Syntax Description

remote-lan-profile-name	Is the remote LAN profile name. Range is from 1 to 32 alphanumeric characters.
rlan-id	Is the remote LAN identifier. Range is from 1 to 128. **Note** You can create a maximum of 128 RLANs. You cannot use the *rlan-id* of an existing RLAN while creating another RLAN. Both RLAN and WLAN profile cannot have the same names. Similarly, RLAN and WLAN policy profile cannot have the same names.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

This example shows how to configure remote LAN profile:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap remote-lan profile-name rlan_profile_name 3
```

ap remote-lan shutdown

To enable or disable all RLANs, use the **ap remote-lan shutdown** command.

ap remote-lan shutdown

Command Default None

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Example

This example shows how to enable or disable all RLANs:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# [no] ap remote-lan shutdown
Device(config)# end
```

ap remote-lan-policy policy-name

To configure RLAN policy profile, use the **ap remote-lan-policy policy-name** command.

ap remote-lan-policy policy-name *profile-name*

Command Default None

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Example

This example shows how to configure RLAN policy profile:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap remote-lan-policy policy-name rlan_policy_prof_name
```

ap reset site-tag

To reboot all the APs associated to a particular site, use the **ap reset site-tag** command.

ap reset site-tag *site-tag-name*

Syntax Description

site-tag-name	Site tag name.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Usage Guidelines

Example

This example shows how to reboot all the APs in a particular site:

```
Device# ap reset site-tag bgl18
```

ap sensor air-pressure

To enable the AP sensor air-pressure data collection for all APs or for specific APs in a site tag, use the **ap sensor air-pressure** {**all** | **site** *site-tag*} [**duration** *duration-time*]

ap sensor air-pressure { **all** | **site** *site-tag* } [**duration** *duration-time*]

Syntax Description

all	Specifies the sensor data collection for all APs.
site *site-tag*	Specifies the sensor data collection for APs in specific site tag.
duration *duration-time*	Specifies the duration for AP sensor data collection. The value range of the duration of the air pressure reporting is between 1 minute and 1440 minutes. The default is 10 minutes. From Cisco IOS XE 17.15.1, the default air pressure sample interval is changed from 30 seconds to 60 seconds. For example, if the duration is set to 10 minutes, the APs send 10 samples spaced at 60 seconds each.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Dublin 17.13.1	This command was introduced.

Examples

The following example shows how to enable the AP sensor air-pressure data collection for all APs or for specific APs in a site tag:

```
Device# ap sensor air-pressure all duration 10
Device# ap sensor air-pressure site sitetag1 duration 10
```

ap tag persistency enable

To configure AP tag persistency settings, use the **ap tag persistency enable** command, in the global configuration mode. To disable the AP tag persistency settings, use the **no** form of this command.

ap tag persistency enable

no ap tag persistency enable

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.6.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows how to enable tag persistency for an AP:

```
Device(config)# ap tag persistency enable
```

ap upgrade method https

To configure AP image download from the controller over HTTPS, use the **ap upgrade method https** command. To remove the upgrade method type, use the **no ap upgrade method https** command.

ap upgrade method https

Syntax Description

https	Specifies HTTPS method for AP image download.

Command Default

AP upgrade method is not set.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Dublin 17.11.1	This command was introduced.

Usage Guidelines

This command works only if the AP supports efficient upgrade method.

Use the **show ap config general** command to check whether the AP supports efficient download method.

Examples

The following example shows how to configure upgrade method for an AP:

```
Device# configure terminal
Device(config)# ap upgrade method https
```

ap upgrade staggered

To configure staggered AP upgrade parameters, use the **ap upgrade staggered** command

ap upgrade staggered { **1** | **2** | **5** | **15** | **25** | **client-deauth** | **client-steering** | **iteration** | **one-shot** | **serial** }

Syntax Description

Keywords and Variables	Description
1	1% of APs per iteration
5	5% of APs per iteration
15	15% of APs per iteration
25	25% of APs per iteration
client-deauth	Enable or disable client de-authentication
client-steering	Enable or disable client steering
iteration	Configure iteration accounting parameters
one-shot	Upgrade all APs in a single iteration
serial	Serialize AP upgrade, one AP per iteration.

Command Default

None

Command Modes

Global Configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.18.1	The **serial** and **1** keywords were introduced.

ap upgrade staggered client-deauth

To deauthenticate the clients connected to an AP when the AP starts to upgrade, use the **ap upgrade staggered client-deauth** command. To disable deauthentication, use the **no** form of this command.

ap upgrade staggered client-deauth

no ap upgrade staggered client-deauth

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Cupertino 17.9.1	This command was introduced.
Cisco IOS XE Dublin 17.11.1	This command was modified. The **no** form of the command was introduced.

Examples

The following example shows how to deauthenticate the clients connected to an AP when the AP starts to upgrade:

```
Device(config)# no ap upgrade staggered client-deauth
```

ap upgrade staggered iteration completion

To configure the minimum percentage of access points (APs) that must join the destination controller to signal iteration completion, use the **ap upgrade staggered iteration completion** command.

ap upgrade staggered iteration completion *min-percent*

Syntax Description

min-percent	Percentage of APs that should join the destination controller. Valid values range from 0 to 100.

Command Default

Minimum percentage is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Cupertino 17.9.1	This command was introduced.

Usage Guidelines

This command helps to configure the minimum percentage of APs that must join the destination controller to signal iteration completion. If APs are not able to join the destination controller, the upgrade is stopped. The overall percentage of missing APs must be less than the percentage configured here at the end of each iteration.

Examples

The following example shows how to configure the minimum percentage of APs that must join back to the network to signal iteration completion:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap upgrade staggered iteration completion 50
```

ap upgrade staggered iteration error

To configure the action to be taken when access points (APs) are missing after an iteration during AP upgrade, use the **ap upgrade staggered iteration error** command.

ap upgrade staggered iteration error action stop

Syntax Description

stop	Specifies the action to be taken when APs are missing after an iteration during AP upgrade.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Cupertino 17.9.1	This command was introduced.

Usage Guidelines

This command allows you to set the action to be taken when the minimum number of APs fail to join the destination controller after an iteration cycle.

For instance, when a site is being upgraded in five iteration cycles, and the fifth one fails because of some error in the destination controller, this command helps you to stop the upgrade.

Examples

The following example shows how to configure the action to be taken when APs fail to join after an iteration during AP upgrade:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap upgrade staggered iteration error action stop
```

ap upgrade staggered iteration timeout

To configure the maximum time allowed per iteration during an access point (AP) upgrade, use the **ap upgrade staggered iteration timeout** command.

ap upgrade staggered iteration timeout *timeout-duration*

Syntax Description

timeout-duration	Time allowed per iteration, in minutes. Valid values range from 9 to 60.

Command Default

Iteration timeout is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Cupertino 17.9.1	This command was introduced.

Usage Guidelines

If an AP upgrade iteration is not completed during the specified duration, the error action that is set using the **ap upgrade staggered iteration error** command is taken.

Examples

The following example shows how to configure the maximum time allowed per iteration:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap upgrade staggered iteration timeout 40
```

ap tag-source-priority

To configure ap tag source priority, use the **ap tag-source-priority** command.

ap tag-source-priority *source-priority* **source** { **filter** | **ap** }

Syntax Description

source-priority	Enter the ap tag source priority. Valid range is 2 to 3.
source	Specifiy the source for which priority is been set.
filter	AP filter as tag source.
ap	AP as tag source.

Command Default

None

Command Modes

config

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to set AP as a tag source:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap tag-source-priority priority-value source ap
```

ap tag-sources revalidate

To revalidate the access point tag sources, use the **ap tag-sources revalidate** command.

ap tag-sources revalidate

Syntax Description

tag-sources	Tag Sources.
revalidate	Revalidate access point tag sources.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to revalidate the access point tag sources:

```
Device# ap tag-sources revalidate
```

ap triradio

To enable or disable tri-radio on all Cisco APs, use the **ap triradio** command.

ap triradio {**disable** | **enable**}

Syntax Description

ap triradio	Enables or disables tri-radio on all Cisco APs.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.2.1	This command was introduced.

Example

The following example shows how to enable or disable tri-radio for all Cisco APs:

```
Device# ap triradio enable
```

ap vlan-tag

To configure VLAN tagging for all nonbridge APs, use the **ap vlan-tag** command.

ap vlan-tag *vlan-id*

Syntax Description

vlan-id	VLAN identifier.

Command Default

VLAN tagging is not enabled for nonbridge APs.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Example

The following example shows how to configure VLAN tagging for all non-bridge APs:

```
Device# ap vlan-tag 1000
```

arp-caching

To enable arp-caching, use the **arp-caching** command.

arp-caching

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

config-wireless-flex-profile

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Example

The following example shows how to enable arp-caching:

```
Device(config-wireless-flex-profile)# arp-caching
```

assisted-roaming

To configure assisted roaming using 802.11k on a WLAN, use the **assisted-roaming** command. To disable assisted roaming, use the **no** form of this command.

assisted-roaming {**dual-list** | **neighbor-list** | **prediction**}

no assisted-roaming {**dual-list** | **neighbor-list** | **prediction**}

Syntax Description

dual-list	Configures a dual band 802.11k neighbor list for a WLAN. The default is the band that the client is currently associated with.
neighbor-list	Configures an 802.11k neighbor list for a WLAN.
prediction	Configures assisted roaming optimization prediction for a WLAN.

Command Default

Neighbor list and dual band support are enabled by default. The default is the band that the client is currently associated with.

Command Modes

WLAN configuration

Usage Guidelines

When you enable the assisted roaming prediction list, a warning appears and load balancing is disabled for the WLAN if load balancing is already enabled on the WLAN. To make changes to the WLAN, the WLAN must be in disabled state.

Example

The following example shows how to configure a 802.11k neighbor list on a WLAN:

```
Device(config-wlan)#assisted-roaming neighbor-list
```

The following example shows the warning message when load balancing is enabled on a WLAN. Load balancing must be disabled if it is already enabled when configuring assisted roaming:

```
Device(config)#wlan test-prediction 2 test-prediction
Device(config-wlan)#client vlan 43
Device(config-wlan)#no security wpa
Device(config-wlan)#load-balance
Device(config-wlan)#assisted-roaming prediction
WARNING: Enabling neighbor list prediction optimization may slow association and impact
VOICE client perform.
Are you sure you want to continue? (y/n)[y]: y
% Request aborted - Must first disable Load Balancing before enabling Assisted Roaming
Prediction Optimization on this WLAN.
```

association-limit

To configure maximum client associations per AP in the AP profile configuration mode, use the **association-limit** command. Use the **no** form of this command to disable the feature.

association-limit *clients-connections*

Syntax Description

client-connections	Configures the maximum number of client connections per AP. The default value is 0. **Note** The maximum clients per AP for Cisco Catalyst 9136 series APs is 1200 clients.

Command Default

None

Command Modes

AP configuration mode

Command History

Release	Modification
Cisco IOS XE Cupertino 17.8.1	This command was introduced.

Example

The following example shows how to configure maximum client associations per AP in the AP profile configuration mode:

```
Device# confiure terminal
Device(config)# ap profile ap-profile-name
Device(config-ap-profile)# association-limit 300
```

attribute type

To define an attribute type that is to be added to an attribute list locally on a device, use the **attribute type** command in global configuration mode. To remove the attribute type from the list, use the **no** form of this command.

attribute type *name value* { [**service** *service*] | [**protocol** *protocol*] | [*tag*] }

Syntax Description

Keywords and Variables	Description
name	The Cisco IOS authentication, authorization, and accounting (AAA) internal name of the IETF RADIUS attribute to be added to the attribute list. For a list of supported attributes, use the CLI help option (?) on your platform.
value	A string, binary, or IPv4 address value. This is the RADIUS attribute that is being defined in Cisco IOS AAA format. A string added to the attribute value must be inside quotation marks. For example, if the value is interface-config and the string is “ip unnumbered FastEthernet0,” you would write interface-config “ip unnumbered FastEthernet0”.
service *service*	(Optional) Specifies the Access method, which is typically PPP.
protocol *protocol*	(Optional) Specifies the type of protocol, which can be ATM, IP, or virtual private Dial-up network (VPDN).
tag	(Optional) A means of grouping attributes that refer to the same VPDN tunnel.

Command Default

None

Command Modes

Global Configuration (config)

Command History

Release	Modification
Cisco IOS XE 17.12.1	This command was introduced in a release earlier than Cisco IOS XE 17.12.1.

Usage Guidelines

Attributes are added to the attribute list each time a new attribute type is defined. Attributes are not validated at configuration. The AAA subsystem recognizes the expected attribute format defined by the services in a definition file. However, it cannot validate the attribute information itself. This validation is done by a service when it first uses the attribute. This validation is applicable to both RADIUS and TACACS+ AAA servers. Thus, if you are not familiar with configuring a AAA server, test your attribute list on a test device with the service that will be using the list before configuring and using it in a production environment.

authentication-type

To configure the 802.11u network authentication type, use the **authentication-type** command. To remove the authentication type, use the **no** form of the command.

authentication-type { **dns-redirect** | **http-https-redirect** [*redirect-url*] | **online-enrollment** | **terms-and-conditions** [*terms*] }

Syntax Description

dns-redirect	Sets the authentication type as DNS redirection.
http-https-redirect	Sets the authentication type as HTTP/HTTPS redirection.
redirect-url	The HTTP/HTTPS redirection URL.
online-enrollment	Sets the authentication type as online enrollment.
terms-and-conditions	Sets the authentication type as terms and conditions.
terms	Terms and conditions URL.

Command Default

None

Command Modes

Wireless ANQP Server Configuration (config-wireless-anqp-server)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

If you use an authentication method, for example, Layer 3 authentication, ensure that you use the same authentication in the WLAN configuration (web authentication).

Example

The following example shows how to configure the 802.11u network authentication type:

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# authentication-type dns-redirect
```

autoqos

To enable Auto QoS wireless policy, use the **autoqos** command. To remove Auto QoS wireless policy, use the **no** form of this command.

autoqos mode { **enterprise-avc** | **fastlane** | **guest** | **voice** }

Syntax Description

enterprise-avc	Enables AutoQos wireless Enterprise policy.
fastlane	Enable AutoQos wireless fastlane policy.
guest	Enables AutoQos wireless guest policy
voice	Enables AutoQos wireless voice policy

Command Default

None

Command Modes

Wireless policy configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

This example shows how to enable AutoQos Wireless Enterprise Policy.

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy policy-test
Device(config-wireless-policy)# autoqos mode enterprise-avc
```

avg-packet-size packetsize

To configure the wireless media-stream's average packet size, use the **avg-packet-size** command.

avg-packet-size *packetsize-value*

Syntax Description

packetsize-value	Average Packet Size. Valid range is 100 to 1500.

Command Default

None

Command Modes

media-stream

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure wireless media-stream's average packet size:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless media-stream group doc-grp 224.0.0.0 224.0.0.223
Device(config-media-stream)# avg-packet-size500
```

avc sd-service

To enable Software-Defined Application Visibility and Control (SD-AVC) service on the controller, use the **avc sd-service** command. To disable SD-AVC service on the controller, use the **no** form of this command.

avc sd-service

no avc sd-service

Syntax Description

This command has no keywords or arguments.

Command Default

SD-AVC service is disabled.

Command Modes

Global Configuration (config)

Command History

Release	Modification
Cisco IOS XE Cupertino 17.7.1	This command was introduced.

Examples

The following example shows how to enable SD-AVC service on the controller:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# avc sd-service
```

avoid label exhaustion error

To avoid label exhaustion error happening on BGP routes during the time period when MSMR and fabric border are on two different nodes and any of those nodes is a catalyst 9300, use the **mpls label mode all-vrfs protocol all-afs per-vrf** command in global configuration mode.

awips

To enable the wireless intrusion threat detection and mitigation mechanism that is known as Advanced Wireless Intrusion Prevention System (aWIPS), use the **awips** command. To disable aWIPS, use the **no** form of the command.

awips [**forensic**]

Syntax Description

forensic	Enables forensics for aWIPS.

Command Default

None

Command Modes

AP Profile Configuration(config-ap-profile)

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.1.1	This command was introduced.
Cisco IOS XE Bengaluru 17.4.1	The **forensic** keyword was added.

Example

The following exmaple shows how to enable aWIPS and forensic.

```
Device# configure terminal
Device(config)#ap profile test
Device(config-ap-profile)#awips
Device(config-ap-profile)#awips forensic
```

awips-syslog

To configure syslog threshold for Cisco Advanced Wireless Intrusion Prevention System (aWIPS), use the **awips-syslog** command. To disable syslog threshold for aWIPS, use the **no** form of this command.

awips-syslog throttle period *value-btwn-30-600-seconds*

Syntax Description

throttle period *value-btwn-30-600-seconds*	Configures the syslog threshold for aWIPS. **Note** The default throttling interval is 60 seconds.	

Command Default

None

Command Modes

Global Configuration

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.6.1	This command was introduced.

Usage Guidelines

This example shows how to configure syslog threshold for aWIPS:

```
Device# configure terminal
Device(config)# awips-syslog throttle period 60
Device(config)# end
```

backhaul (mesh)

To configure mesh backhaul for a mesh AP profile, use the **backhaul** command.

backhaul rate dot11 {**24ghz** | **5ghz**} {**auto** | **dot11abg** *rate* | **dot11n mcs** *mcs-index* }

Syntax Description

rate	Backhaul transmission rate.
dot11	Specifies 802.11.
24ghz	Specifies 802.11b.
5ghz	Specifies 802.11a.
auto	Specifies method as auto.
dot11abg	Specifies method as dot11abg.
dot11n	Specifies method as dot11n.
mcs	Media convergence servers.
rate	Media convergence server rate.
mcs-index	Media convergence servers rate value for 802.11.

Command Default

Backhaul client access is disabled.

Command Modes

config-wireless-mesh-profile

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Example

The following example shows how to configure mesh backhaul details for a mesh AP profile:

```
Device # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device (config)# wireless profile mesh mesh-profile
Device (config-wireless-mesh-profile)# backhaul rate dot11 24ghz auto
```

background-scanning (mesh)

To configure background scanning for a mesh AP profile, use the **background-scanning** command.

background-scanning

Syntax Description

This command has no keywords or arguments.

Command Default

Background scanning is disabled.

Command Modes

config-wireless-mesh-profile

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Example

The following example shows how to configure background scanning for a mesh AP profile:

```
Device # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device (config)# wireless profile mesh mesh-profile
Device (config-wireless-mesh-profile)# background-scanning
```

band-select client

To configure the client threshold minimum dB for the selected band, use the **band-select client** command. To reset the client threshold minimum dB for the selected band, use the **no** form of this command.

band-select client { **mid-rssi** | **rssi** } *dBm value*

Syntax Description

mid-rssi	Minimum dBm of a client RSSI start to respond to probe
rssi	Minimum dBm of a client RSSI to respond to probe
dBm value	Minimum dBm of a client RSSI to respond to probe. Valid range is between –90 and –20 dBm.

Command Default

None

Command Modes

config-rf-profile

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines

This command is enabled only for 2.4-GHz band.

This example shows how to set the client threshold to minimum dB for a selected band.

```
Device(config-rf-profile)#band-select client rssi -50
```

band-select cycle

To configure the band cycle parameters, use the **band-select cycle** command. To reset the threshold value, use the **no** form of this command.

band-select cycle { **count** | **threshold** } *value*

Syntax Description

count	Sets the Band Select probe cycle count.
value	Maximum number of cycles not responding. The range is between 1 and 10.
threshold	Sets the time threshold for a new scanning cycle.
value	Set the threshold value in milliseconds. The valid is between 1and 1000.

Command Default

None

Command Modes

config-rf-profile

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines

None

This example shows how to configure the probe cycle count in an RF profile for a selected band.

```
Device(config-rf-profile)#band-select cycle count 5
```

band-select expire

To configure the expiry time for the RF profile for the selected band, use the **band-select expire** command. To reset the value, use the **no** form of this command.

band-select expire { **dual-band** | **suppression** } *value*
no band-select expire { **dual-band** | **suppression** }

Syntax Description

dual-band	Configures the RF Profile Band Select Expire Dual Band.
value	Setting the time to expire for pruning previously known dual-band clients. The range is between 10 and 300.
suppression	Configures the RF Profile Band Select Expire Suppression.
value	Setting the time to expire for pruning previously known 802.11b/g clients. The range is between 10 and 200.

Command Default

None

Command Modes

config-rf-profile

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines

None

This example shows how to configure the time to expire for a dual-band of an RF profile in a selected band.

```
Device(config-rf-profile)#band-select expire dual-band 15
```

band-select probe-response

To configure the probe responses to the clients for a selected band, use the **band-select probe-response** command. To disable the probe-response, use the **no** form of this command.

band-select probe-response

Syntax Description

probe-response	Probe responses to clients.

Command Default

None

Command Modes

config-rf-profile

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines

None

This example shows how to enable probe response to the clients.

```
Device(config-rf-profile)#band-select probe-response
```

banner text

To configure the message in a banner, use the **banner text** command. Use the **no** form of this command to remove the message.

banner text *text*

no banner text

Syntax Description

text	Text message to be displayed.

Command Default

None

Command Modes

Parameter map configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure a message in a banner:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# parameter-map type webauth global
Device(config-params-parameter-map)# banner text #Hêllö#
```

battery-state (mesh)

To configure battery state for an AP, use the **battery-state** command.

battery-state

Syntax Description

This command has no keywords or arguments.

Command Default

Battery state is enabled.

Command Modes

config-wireless-mesh-profile

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Example

The following example shows how to configure battery state for an AP:

```
Device # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device (config)# wireless profile mesh mesh-profile
Device (config-wireless-mesh-profile)# battery-state
```

boot system flash

To configure boot system flash parameters, use the **boot system flash** command. To remove boot system flash parameters, use the **no** form of the command.

boot system flash { **bootflash:** | **harddisk:** | **usb:** | **cns:** | **crashinfo:** | **flash:** | **null:** | **nvram:** | **system:** | **tar:** | **tmpsys:** | **webui:** } *options*

Syntax Description

bootflash:	Enables directory or file name.
harddisk:	Enables directory or file name.
usb:	Enables directory or file name.
cns:	Enables directory. This URL prefix accepts no filename
crashinfo:	Enables directory or file name.
flash:	Enables directory or file name.
null:	Enables directory. This URL prefix accepts no filename
nvram:	Enables directory or file name.
system:	Enables directory or file name.
tar:	Enables directory or file name.
tmpsys:	Enables directory or file name.
webui:	Enables directory or file name.
options	System image file name.

Command Default

None

Command Modes

Global Configuration (config)

Command History

Release	Modification
Cisco IOS XE Cupertino 17.8.1	This command was introduced.

Usage Guidelines

You can use the auto-complete feature using a few letters of the keyword and the tab key. For example, **boot system flash boot** and tab key displays **boot system flash bootflash:** command. The auto-complete feature works only for the local file system.

You can use the '?' option to display files in the system. For example, **boot system flash bootflash:?** will display all the associated files for the command.

If the file name you enter is not present locally, the following error is displayed.

```
Device(config)#boot system flash bootflash:abc.bin
%Error parsing bootflash:/abc.bin (No such file or directory)
```

Example

The following example shows how to configure boot system flash parameters:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# boot system flash
bootflash:C9800-CL-rpboot.BLD_V178_THROTTLE_LATEST_20220111_082010.SSA.pkg
```

bridge-group

To configure bridge group parameters for a mesh AP profile, use the **bridge-group** command.

bridge-group {**name** *bridge-group-name* | **strict-match** }

Syntax Description

name *bridge-group-name*	Configures bridge group name.
strict-match	Configures bridge group strict matching.

Command Default

None

Command Modes

config-wireless-mesh-profile

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure the bridge group name for a mesh AP profile:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile mesh mesh-profile
Device(config-wireless-mesh-profile)# bridge-group name mesh-bridge-group
```

bss-transition

To configure BSS transition per WLAN, use the **bss-transition** command.

bss-transition [**disassociation-imminent**]

Syntax Description

disassociation-imminent	BSS transition disassociation Imminent per WLAN.

Command Default

None

Command Modes

config-wlan

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Example

The following example shows how to configure BSS transition per WLAN:

```
Device(config-wlan)# bss-transition
```

bssid-stats bssid-stats frequency

To set the frequency timer of BSSID statistics, use the **bssid-stats bssid-stats frequency** command. To disable the timer, use the **no** form of the command.

bssid-stats bssid-stats frequency *<timer value>*

[no] bssid-stats bssid-stats frequency

Syntax Description

bssid-stats frequency	Sets the frequency timer of BSSID statistics in seconds.
<1-180>	Sets the frequency value between the range of 1 to 180 seconds.

Command Default

None

Command Modes

AP profile configuration

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.2.1	This command was introduced.

Example

This example shows how to set the frequency timer of BSSID statistics:

```
Device(config-ap-profile)#bssid-stats bssid-stats-frequency 100
```

bssid-neighbor-stats interval

To enable the BSSID neighbor statistics and to set the interval (in seconds) at which BSSID neighbor statistics will be sent from the AP, use the **bssid-neighbor-stats interval** command. To disable the feature, use the **no** form of the command.

bssid-neighbor-stats interval *bssid-neighbor-stats-interval*

[no] bssid-neighbor-stats interval *bssid-neighbor-stats-interval*

Syntax Description

bssid-neighbor-stats	Enables or disables BSSID neighbor statistics.
interval	Sets the interval in seconds at which BSSID neighbor statistics will be send from the AP.
bssid-neighbor-stats-interval	Specifies the interval in seconds at which BSSID neighbor statistics will be send from the AP. The value ranges from 30 to 600 seconds. The default value is 180 seconds.

Command Default

None

Command Modes

AP Profile configuration mode

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.2.1	This command was introduced.

Example

To show the BSSID neighbor statistics interval being set in seconds:

```
Device(config-ap-profile)#bssid-neighbor-stats interval 90
```

bucket

To configure a bucket for storing objects and its mounting point in Amazon S3, use the **bucket** command. To remove the bucket and its mounting point, use the **no** form of the command.

bucket *bucket-name* **mount-point** *mount-point*

no bucket *bucket-name* **mount-point** *mount-point*

Syntax Description

bucket-name	Amazon S3 storage bucket.
mount-point	Amazon S3 mount point.

Command Default

Storage bucket and mount point are not configured.

Command Modes

S3fs Profile Configuration (config-s3fs-profile)

Command History

Release	Modification
Cisco IOS XE 17.13.1	This command was introduced.

Usage Guidelines

S3fs-fuse is an agent implementation that allows Amazon S3 storage buckets to be accessed as part of the Linux file system. By utilizing Amazon S3 APIs and Linux FUSE infrastructure, each instance of an Amazon S3 bucket can be mounted onto a designated directory in the device's file system. To support the essential functionality of making Amazon S3 buckets available on the device's file system, S3fs-fuse is integrated into the IOS-XE SDK.

Examples

The following example shows how to configure a bucket for storing objects and its mounting point.

```
Device# configure terminal
Device(config)# cloud-services aws s3 profile 9800_XT_HD
Device(config-s3fs-profile)# bucket 9800-B1 mount-point s3-mount
```

cache timeout active value

To set the active flow monitor timeout value in seconds, use the **cache timeout active value** command.

cache timeout active *value*

Syntax Description

value	Enter the active timeout value. Valid range is 1 to 604800.

Command Default

None

Command Modes

config-flow-monitor

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to set the flow monitor inactive timeout value:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# flow monitor flow-monitor-name
Device(config-flow-monitor)# cache timeout active 300
```

cache timeout inactive value

To set the flow monitor inactive timeout value in seconds, use the **cache timeout inactive value** command.

cache timeout inactive *value*

Syntax Description

value	Enter the inactive timeout value. Valid range is 1 to 604800.

Command Default

None

Command Modes

config-flow-monitor

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to set the flow monitor inactive timeout value:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# flow monitor flow-monitor-name
Device(config-flow-monitor)# cache timeout inactive 300
```

call-snoop

call-snoop

no call-snoop

Syntax Description

This command has no keywords or arguments.

Command Default

VoIP snooping is disabled by default.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command. The WLAN on which call snooping is configured must be configured with Platinum QoS. You must disable quality of service before using this command.

Example

This example shows how to enable VoIP on a WLAN:

```
Device# configure terminal
Device(config)# wireless profile policy policy-name
Device(config-wireless-policy)#service-policy input platinum-up
Device(config-wireless-policy)#service-policy output platinum
Device(config-wireless-policy)#call-snoop
Device(config-wireless-policy)#no shutdown
Device(config-wireless-policy)#end
```

calender-profile name

To map a calender profile to a policy profile, use the **calender-profile name** command.

calender-profile name *calendar-profile-name*

Syntax Description

calendar-profile-name	Specifies the name of the calendar profile name.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

This example shows how to map a calender profile to a policy profile:

```
Device# configure terminal
Device(config)# wireless profile policy default-policy-profile
Device(config-wireless-policy)# calender-profile name daily_calendar_profile
Device(config-policy-profile-calender)# action deny-client
Device(config-policy-profile-calender)# end
```

captive-bypass-portal

To configure captive bypassing, use the **captive-bypass-portal** command.

captive-bypass-portal

Command Default None

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Example

This example shows how to configure captive bypassing for WLAN in LWA and CWA:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# parameter-map type webauth WLAN1_MAP
Device(config)# captive-bypass-portal
Device(config)# wlan WLAN1_NAME 4 WLAN1_NAME
Device(config-wlan)# security web-auth
Device(config-wlan)# security web-auth parameter-map WLAN1_MAP
Device(config-wlan)# end
```

capwap-discovery

To set CAPWAP discovery response method as to whether a capwap-discovery response contains the public or private IP of the controller, use the **capwap-discovery** command.

capwap-discovery { **private** | **public** }

Syntax Description

private	Includes private IP in CAPWAP discovery response.
public	Includes public IP in CAPWAP discovery response.

Command Default

None

Command Modes

Management Interface Configuration(config-mgmt-interface)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Usage Guidelines

Example

The following example shows how to configure a CAPWAP discovery response method:

```
Device# configure terminal
Device(config)# wireless management interface Vlan1
Device(config-mgmt-interface)# capwap-discovery public
```

capwap aggregation

To enable CAPWAP message aggregation in the controller, use the **capwap aggregation** command. To disable the functionality, use the **no** form of this command.

capwap aggregation

no capwap aggregation

Syntax Description

This command has no keywords and arguments.

Command Default

The CAPWAP Message Aggregation feature is disabled by default.

Command Modes

config-ap-profile

Command History

Release	Modification
Cisco IOS XE 17.14.1	This command was introduced.

Usage Guidelines

The CAPWAP Message Aggregation feature aggregates the CAPWAP control messages to be sent to APs. When APs are busy processing packets, the messages to be sent to the APs are stored in the controller. When you enable the feature, if the last message type in the queue and the current message type are the same, the CAPWAP messages are aggregated and capped at Maximum Transmission Unit (MTU). This improves the performance of the system.

Examples

This example shows how to enable CAPWAP message aggregation in the controller:

```
Device# configure terminal
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# capwap aggregation
Device(config-ap-profile)# end
```

capwap backup

To configure a primary or secondary backup device for all access points that are joined to a specific device, use the **capwap backup** command.

capwap backup {**primary** *primary-controller-name primary-controller-ip-address* | **secondary** *secondary-controller-name secondary-controller-ip-address*}

Syntax Description

primary	Specifies the primary backup device.
primary-controller-name	Primary backup device name.
primary-controller-ip-address	Primary backup device IP address.
secondary	Specifies the secondary backup device.
secondary-controller-name	Secondary backup device name.
secondary-controller-ip-address	Secondary backup device IP address.

Command Default

None

Command Modes

AP profile configuration (config-ap-profile)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

This example shows how to configure a primary backup device for all access points that are joined to a specific device:

```
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# capwap backup primary controller1 192.0.2.51
```

This example shows how to configure a secondary backup device for all access points that are joined to a specific device:

```
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# capwap backup secondary controller1 192.0.2.52
```

capwap window size

To configure AP CAPWAP control packet transmit queue size, use the **capwap window size** command. To reset the AP CAPWAP control packet transmit queue size to default level, use the **no** form of the command.

capwap window size *window-size*

Syntax Description

window-size	AP CAPWAP control packet transmit queue size. The valid range is from 1 to 50, with the default value of 1. We recommend that you limit the maximum value to 20.

Note For standard AP deployments, retain the default CAPWAP window size of `1`. Configure a higher value only for AP profiles used exclusively for Teleworker or OfficeExtend APs. If APs repeatedly disconnect and rejoin the controller or experience CAPWAP keepalive timeouts, reset the value to `1` using `no capwap window size` or `capwap window size 1`.

Command Default

None

Command Modes

AP profile configuration (config-ap-profile)

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.3.1	This command was introduced.

Example

The following example shows how to configure the AP CAPWAP control packet transmit queue size:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# capwap window size 20
```

capwap udplite

To enable IPv6 CAPWAP UDP Lite on Cisco APs, use the **capwap udplite** command.

Note You get to view the following message:

This feature is supported only for IPv6 data packets, APs will be rebooted.

capwap udplite

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.1.1s	This command was introduced.

This example shows how to enable IPv6 CAPWAP UDP Lite on Cisco APs:

```
Device# configure terminal
Device (config)# ap profile default-ap-profile
Device (config-ap-profile)# capwap udplite
Device (config-ap-profile)# end
```

ccn (mesh)

To configure channel change notification for a mesh AP profile, use the **ccn** command.

ccn

Syntax Description

This command has no keywords or arguments.

Command Default

Channel change notification is disabled.

Command Modes

config-wireless-mesh-profile

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Example

The following example shows how to configure channel change notification for a mesh AP profile:

```
Device # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device (config)# wireless profile mesh mesh-profile
Device (config-wireless-mesh-profile)# ccn
```

ccx aironet-iesupport

To configure the support of Aironet IE CCX option, use the following command:

ccx aironet-iesupport

Syntax Description

ccx	Configures the Cisco Client Extension options.
aironet-iesupport	Sets the support of Aironet IE on WLAN.

Command Default

None

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.2.1	This command was introduced.

Example

This example shows how to configure Aironet IE support:

```
Device(config-wlan)#ccx aironet-iesupport
```

cdp

To enable the Cisco Discovery Protocol (CDP) on a Cisco lightweight access point under the AP profile, use the **cdp** command. To disable the Cisco Discovery Protocol (CDP) on a Cisco lightweight access point, use the **no** form of this command.

```
ap profile default-ap-profile

cdp
no  cdp
```

Command Default Disabled on all access points.

Command Modes AP profile mode (config-ap-profile)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines The **no cdp** command disables CDP on all access points that are joined to the device and all access points that join in the future. CDP remains disabled on both current and future access points even after the device or access point reboots. To enable CDP, enter the **cdp** command.

Note CDP over Ethernet/radio interfaces is available only when CDP is enabled.

This example shows how to enable CDP on all access points:

```
Device(config)# ap profile default-ap-profile


Device(config-ap-profile)# cdp
```

central authentication

To enable or disable central authentication, use the **central authentication** command.

central authentication

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

config-wireless-policy

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Example

The following example shows how to enable central authentication:

```
Device(config-wireless-policy)# central authentication
```

central dhcp

To enable central dhcp for locally switched clients, use the **central dhcp** command.

central dhcp

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

config-wireless-policy

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Example

The following example shows how to enable central dhcp for locally switched clients:

```
Device(config-wireless-policy)# central dhcp
```

central switching

To enable or disable central switching, use the **central switching** command.

central switching

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

config-wireless-policy

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Example

The following example shows how to enable or disable central switching:

```
Device(config-wireless-policy)# central switching
```

central-webauth

To configure central-webauth for an ACL, use the **central-webauth** command.

central-webauth

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

config-wireless-policy

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Example

The following example shows how to configure central-webauth for an ACL:

```
Device(config-wireless-policy)# central-webauth
```

channel unii3-low-power-channels

To enable UNII-3 low power channels for 802.11a in the RF profile, use the **channel unii3-low-power-channels** command.

channel unii3-low-power-channels

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

RF profile configuration (config-rf-profile)

Command History

Release	Modification
Cisco IOS XE Dublin 17.17.1	This command was introduced.

Usage Guidelines

The UNII-3-low-power-channels is applicable only for 5-GHz band.

Examples

The following example shows how to enable UNII-3 low power channels for 802.11a in the RF profile:

```
Device# configure terminal
Device(config)# ap dot11 5ghz rf-profile ax-profile
Device(config-rf-profile)# channel unii3-low-power-channels
```

chassis redundancy ha-interface

To configure the high availability (HA) interface for a chassis, use the **chassis redundancy ha-interface** command.

Note This command is not applicable for Cisco Catalyst CW9800H1 and CW9800H2, and CW9800M Wireless Controllers as they do not support RP only SSO deployment.

chassis redundancy ha-interface GigabitEthernet*interface-number* **local-ip** *ip-address netmask* **remote-ip** *remote-chassis-ip-addr*

Syntax Description

interface-number	GigabitEthernet interface number. Valid range is 1 to 32.
local-ip *ip-address netmask*	Configures the IP address of the local chassis HA interface. For the netmask, enter the netmask or the prefix length in the following formats: */nn* or *A.B.C.D*.
remote-ip *remote-chassis-ip-addr*	Configures the remote chassis IP address.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure the HA interface for a chassis:

```
Device# chassis ha-interface GigabitEthernet 2 local-ip 10.10.10.10 255.255.255.0 remote-ip
 10.10.10.11
```

chassis redundancy ha-interface GigabitEthernet

To create an HA interface for your controller, use the **chassis redundancy ha-interface GigabitEthernet** command.

Note This command is applicable only for Cisco Catalyst 9800 Series Wireless Controllers.

chassis redundancy ha-interface GigabitEthernet *num*

Syntax Description

num	GigabitEthernet interface number. Valid range is 1 to 32.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

This example shows how to create an HA interface for your controller:

```
Device# chassis redundancy ha-interface GigabitEthernet 3
```

chassis redundancy ha-interface shutdown

To configure [no] shutdown of ha_port interface to support RMA, use the **chassis redundancy ha-interface shutdown** command.

Syntax Description

Device# chassis redundancy ha-interface shutdown	Redundancy interface shutdown.

Command Default:

[no] chassis redundancy ha-interface shutdown

Command Modes

This is an exec CLI

Command History

Release	Modification
Cisco IOS XE 17.12	This command was introduced in the release Cisco IOS XE 17.12.

Examples

The following example shows how to configure [no] shutdown of ha_port interface to support RMA:

```
Device# chassis redundancy ha-interface shutdown
```

chassis redundancy keep-alive

To configure peer keep-alive retries and time interval before claiming peer is down, use the **chassis redundancy keep-alive** command.

chassis redundancy keep-alive { **retries** *retries* | **timer** *timer* }

Syntax Description

retries	Chassis peer keep-alive retries before claiming peer is down. Valid values range from 5 to 10, enter 5 for default.
timer	Chassis peer keep-alive time interval in multiple of 100 ms. Valid values range from 1 to 10, enter 1 for default.

Command Default

None

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure peer keep-alive retries and time interval:

```
Device# chassis redundancy keep-alive retries 6
Device# chassis redundancy keep-alive timer 6
```

chassis renumber

To renumber the local chassis id assignment, use the **chassis renumber** command.

chassis *chassis-num* **renumber** *renumber-id*

Syntax Description

chassis-num	Chassis number.
renumber-id	Local chassis id.

Command Default

None

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to renumber the local chassis id assignment:

```
Device# chassis 1 renumber 1
```

chassis priority

To set the priority of the specified device, use the **chassis priority** command.

chassis *chassis-num* **priority** *priority-id*

Syntax Description

chassis-num	Chassis number.
priority-id	Chassis priority.

Command Default

None

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to set the priority of the specified device:

```
Device# chassis 1 priority 1
```

chassis transport

To enable or disable chassis transport, use the **chassis transport** command.

chassis *chassis-num* **transport** {**enable** | **disable**}

Syntax Description

chassis-num	Chassis number.

Command Default

None

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to enable chassis transport:

```
Device# chassis 1 transport enable
```

ciphersuite

To configure the ciphersuites for syslog connection, use the **cyphersuite** command. You can specify one or more ciphersuites.

cyphersuite { **aes-256-cbc-sha** | **aes-128-cbc-sha** | **dhe-aes-cbc-sha2** | **dhe-aes-gcm-sha2** | **ecdhe-ecdsa-aes-gcm-sha2** | | **ecdhe-rsa-aes-cbc-sha2** | **ecdhe-rsa-aes-gcm-sha2** | **rsa-aes-cbc-sha2** | **rsa-aes-gcm-sha2** | **tls13-aes128-gcm-sha256** | **tls13-aes256-gcm-sha384** | **tls13-chacha20-poly1305-sha256** }

Syntax Description

aes-256-cbc-sha	Specifies the encryption type as tls_rsa_with_aes_cbc_256_sha ciphersuite
aes-128-cbc-sha	Specifies the encryption type as tls_rsa_with_aes_cbc_128_sha ciphersuite.
dhe-aes-cbc-sha2	Specifies the encryption type as tls_dhe_rsa_with_aes_cbc_sha2 (TLS1.2) ciphersuite.
dhe-aes-gcm-sha2	Specifies the encryption type as tls_dhe_rsa_with_aes_gcm_sha2 (TLS1.2) ciphersuite.
ecdhe-ecdsa-aes-gcm-sha2	Specifies the encryption type as tls_ecdhe_ecdsa_aes_gcm_sha2 (TLS1.2) SuiteB ciphersuite.
ecdhe-rsa-aes-cbc-sha2	Specifies the encryption type as tls_ecdhe_rsa_aes_cbc_sha2 (TLS1.2) ciphersuite.
ecdhe-rsa-aes-gcm-sha2	Specifies the encryption type as tls_ecdhe_rsa_aes_gcm_sha2 (TLS1.2) ciphersuite.
rsa-aes-cbc-sha2	Specifies the encryption type as tls_rsa_with_aes_cbc_sha2 (TLS1.2) ciphersuite.
rsa-aes-gcm-sha2	Specifies the encryption type as tls_rsa_with_aes_gcm_sha2 (TLS1.2) ciphersuite.
tls13-aes128-gcm-sha256	Specifies the encryption type as tls13_aes128_gcm_sha256 (TLS1.3) ciphersuite.
tls13-aes256-gcm-sha384	Specifies the encryption type as tls13_aes256_gcm_sha384 (TLS1.3) ciphersuite.
tls13-chacha20-poly1305-sha256	Specifies the encryption type as tls13_chacha20_poly1305_sha256 (TLS1.3) ciphersuite.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 17.18.2	This command was introduced.

Examples

The following example shows you how to configure the ciphersuites for syslog connection:

```
Device(config)# logging tls-profile tls-profile-name
Device(config-tls-profile)# ciphersuite aes-256-cbc-sha dhe-aes-cbc-sha2
```

cisco-dna grpc

To enable gRPC channel on Cisco DNA, use the **cisco-dna grpc** command. To disable the configuration, use the no form of the command.

cisco-dna grpc

no cisco-dna grpc

Syntax Description

grpc	Enables gRPC channel on Cisco DNA.

Command Default

None

Command Modes

AP Profile configuration mode

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.3.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows how to enable gRPC channel on Cisco DNA :

```
Device(config-ap-profile)# cisco-dna grpc
```

class

To define a traffic classification match criteria for the specified class-map name, use the **class** command in policy-map configuration mode. Use the **no** form of this command to delete an existing class map.

class {*class-map-name* | **class-default**}
no class {*class-map-name* | **class-default**}

Syntax Description

class-map-name	The class map name.
class-default	Refers to a system default class that matches unclassified packets.

Command Default

No policy map class-maps are defined.

Command Modes

Policy-map configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

Before using the **class** command, you must use the **policy-map** global configuration command to identify the policy map and enter policy-map configuration mode. After specifying a policy map, you can configure a policy for new classes or modify a policy for any existing classes in that policy map. You attach the policy map to a port by using the **service-policy** interface configuration command.

After entering the **class** command, you enter the policy-map class configuration mode. These configuration commands are available:

- **admit**—Admits a request for Call Admission Control (CAC)
- **bandwidth**—Specifies the bandwidth allocated to the class.
- **exit**—Exits the policy-map class configuration mode and returns to policy-map configuration mode.
- **no**—Returns a command to its default setting.
- **police**—Defines a policer or aggregate policer for the classified traffic. The policer specifies the bandwidth limitations and the action to take when the limits are exceeded. For more information about this command, see *Cisco IOS Quality of Service Solutions Command Reference* available on Cisco.com.
- **priority**—Assigns scheduling priority to a class of traffic belonging to a policy map.
- **queue-buffers**—Configures the queue buffer for the class.
- **queue-limit**—Specifies the maximum number of packets the queue can hold for a class policy configured in a policy map.
- **service-policy**—Configures a QoS service policy.
- **set**—Specifies a value to be assigned to the classified traffic. For more information, see set
- **shape**—Specifies average or peak rate traffic shaping. For more information about this command, see *Cisco IOS Quality of Service Solutions Command Reference* available on Cisco.com.

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

The **class** command performs the same function as the **class-map** global configuration command. Use the **class** command when a new classification, which is not shared with any other ports, is needed. Use the **class-map** command when the map is shared among many ports.

You can configure a default class by using the **class class-default** policy-map configuration command. Unclassified traffic (traffic that does not meet the match criteria specified in the traffic classes) is treated as default traffic.

You can verify your settings by entering the **show policy-map** privileged EXEC command.

Examples

This example shows how to create a policy map called policy1. When attached to the ingress direction, it matches all the incoming traffic defined in class1, sets the IP Differentiated Services Code Point (DSCP) to 10, and polices the traffic at an average rate of 1 Mb/s and bursts at 20 KB. Traffic exceeding the profile is marked down to a DSCP value gotten from the policed-DSCP map and then sent.

```
Device(config)# policy-map policy1
Device(config-pmap)# class class1
Device(config-pmap-c)# set dscp 10
Device(config-pmap-c)# police 1000000 20000 conform-action
Device(config-pmap-c)# police 1000000 20000 exceed-action
Device(config-pmap-c)# exit
```

This example shows how to configure a default traffic class to a policy map. It also shows how the default traffic class is automatically placed at the end of policy-map pm3 even though **class-default** was configured first:

```
Device# configure terminal
Device(config)# class-map cm-3
Device(config-cmap)# match ip dscp 30
Device(config-cmap)# exit

Device(config)# class-map cm-4
Device(config-cmap)# match ip dscp 40
Device(config-cmap)# exit

Device(config)# policy-map pm3
Device(config-pmap)# class class-default
Device(config-pmap-c)# set dscp 10
Device(config-pmap-c)# exit

Device(config-pmap)# class cm-3
Device(config-pmap-c)# set dscp 4
Device(config-pmap-c)# exit

Device(config-pmap)# class cm-4
Device(config-pmap-c)# set precedence 5
Device(config-pmap-c)# exit
Device(config-pmap)# exit

Device# show policy-map pm3
Policy Map pm3
  Class cm-3
    set dscp 4
  Class cm-4
    set precedence 5
```

```
Class class-default
  set dscp af11
```

classify

To classify a rule for rogue devices, use the **classify** command.

classify {**friendly** | **malicious** | **delete**}

Syntax Description

friendly	Classifies devices matching this rule as friendly.
malicious	Classifies devices matching this rule as malicious.
delete	Devices matching this rule are ignored.

Command Default

None

Command Modes

config-rule

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to classify rogue devices as friendly:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless wps rogue rule my-rogue-rule priority 3
Device(config-rule)# classify friendly
```

class-map

To create a class map to be used for matching packets to the class whose name you specify and to enter class-map configuration mode, use the **class-map** command in global configuration mode. Use the **no** form of this command to delete an existing class map and to return to global or policy map configuration mode.

class-map [**match-any***type*][**match-all***type*] *class-map-name*
no class-map [**match-any***type*][**match-all***type*] *class-map-name*

Syntax Description

match-any	(Optional) Performs a logical-OR of the matching statements under this class map. One or more criteria must be matched.
type	(Optional) Configures the CPL class map.
class-map-name	The class map name.

Command Default

No class maps are defined.

Command Modes

Global configuration

Policy map configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
	The **type** keyword was added.

Usage Guidelines

Use this command to specify the name of the class for which you want to create or modify class-map match criteria and to enter class-map configuration mode.

The **class-map** command and its subcommands are used to define packet classification, marking, and aggregate policing as part of a globally named service policy applied on a per-port basis.

After you are in quality of service (QoS) class-map configuration mode, these configuration commands are available:

- **description**—Describes the class map (up to 200 characters). The **show class-map** privileged EXEC command displays the description and the name of the class map.
- **exit**—Exits from QoS class-map configuration mode.
- **match**—Configures classification criteria.
- **no**—Removes a match statement from a class map.

If you enter the **match-any** keyword, you can only use it to specify an extended named access control list (ACL) with the **match access-group** class-map configuration command.

To define packet classification on a physical-port basis, only one **match** command per class map is supported.

The ACL can have multiple access control entries (ACEs).

Examples

This example shows how to configure the class map called class1 with one match criterion, which is an access list called 103:

```
Device(config)# access-list 103 permit ip any any dscp 10
Device(config)# class-map class1
Device(config-cmap)# match access-group 103
Device(config-cmap)# exit
```

This example shows how to delete the class map class1:

```
Device(config)# no class-map class1
```

You can verify your settings by entering the **show class-map** privileged EXEC command.

clear aaa counters servers radius

To clear all AAA server radius or specific server radius, use the **clear aaa counters servers radius** {*server-id* | **all**}

clear aaa counters servers radius { *server-id* | **all** }

Syntax Description

server-id	Specifies the server IDs of the AAA servers that are displayed by the **show** command.
all	Specifies all the AAA server IDs.

Command Default

None

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Example

The following example shows how to clear all AAA server radius:

```
Device# clear aaa counters servers radius all
```

clear ap config

To securely erase files from the file system of the Cisco Access Points, use the **clear ap config** command.

clear ap config *ap-name*

Syntax Description

ap-name	Name of the access point.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Dublin 17.11.1.	This command was introduced.

Usage Guidelines

This command needs to be run on the AP console.

Example

The following example shows to trigger a data wipe on the AP:

```
Device# clear ap config doc-test
```

clear ap geolocation ranging site

To clear or purge the AP geolocation Fine Time Measurement (FTM) report for all APs in a site, use the **clear ap geolocation ranging site** *site-tag* command.

clear ap geolocation ranging site *site-tag*

Syntax Description

site-tag	Specifies the name of the site-tag from which the FTM report for the APs in the specified site is cleared.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Dublin 17.13.1	This command was introduced.

Examples

The following example shows how to clear or purge the AP geolocation Fine Time Measurement (FTM) report for all APs in a site:

```
Device# clear ap geolocation ranging site sitetag1
```

clear ap meraki stats

To clear Meraki AP related data, use the **clear ap meraki stats** command.

clear ap meraki stats

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Cupertino 17.9.1	This command was introduced.

Example

This example shows how to clear Meraki AP related data:

```
Device# clear ap meraki stats
```

clear ap sort statistics

To clear the sorted AP statistics, use the **clear ap sort statistics** command.

clear ap sort statistics

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.1.1s	This command was introduced.

This example shows how to clear the sorted AP statistics:

```
Device# clear ap sort statistics
```

clear chassis redundancy

To clear high-availability (HA) configuration, use the **clear chassis redundancy** command.

clear chassis redundancy

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to clear HA configuration:

```
Device# clear chassis redundancy
```

clear ip nbar protocol-discovery wlan

To clear the NBAR2 protocol discovery statistics on a specific WLAN, use the **clear ip nbar protocol-discovery wlan** command.

clear ip nbar protocol-discovery wlan *wlan-name*

Syntax Description

wlan-name	Enter the WLAN name.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to clear the NBAR protocol discovery statistics on a perticular WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# clear ip nbar protocol-discovery wlan wlan-name
```

clear mdns-sd statistics

To clear mDNS statistics, use the **clear mdns-sd statistics** command.

clear mdns-sd statistics { **debug** | **glan-id** *<1 - 5>* | **rlan-id** *<1 - 128>* **wired** | **wlan-id** *<1 - 4096>* }

Syntax Description

debug	Clears the mDNS debug statistics.
glan-id*<1 - 5>*	Clears the GLAN ID. The value range is from 1 to 5.
rlan-id*<1 - 128>*	Clears the RLAN ID. The value range is from 1 to 128.
wired	Clears the mDNS wired statistics.
wlan-id*<1 - 4096>*	Clears the WLAN ID. The value range is from 1 to 4096.

Command Default

None

Command Modes

Privileged EXEC mode

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.3.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows how to clear the mDNS statistics:

```
Device# clear mdns-sd statistics
```

clear platform condition all

To clear all conditional debug and packet-trace configuration and data, use the **clear platform condition all** command.

clear platform condition all

Command Default None

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to clear all conditional debug and packet-trace configuration and data:

```
Device# clear platform condition all
```

clear platform hardware chassis active qfp feature wireless trace-buffer ingress

To clear QFP wireless ingress packet filtered trace and global trace, use the **clear platform hardware chassis active qfp feature wireless trace-buffer ingress** command.

clear platform hardware chassis active qfp feature wireless trace-buffer ingress { **all** | **conditions** | **filtered-trace** | **global-trace** }

Syntax Description

all	Clears conditions, global trace buffer, and filtered-trace buffer.
conditions	Clears all filtered-trace conditions.
filtered-trace	Clears filtered trace buffer.
global-trace	Clears global trace buffer.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.6.1	This command was introduced.

Example

The following example shows you how to clear QFP wireless ingress packet filtered trace:

```
Device# clear platform hardware chassis active qfp feature wireless trace-buffer ingress
all
```

clear platform hardware chassis active qfp feature wireless trace-buffer punt-inject

To clear QFP wireless punt-inject filtered trace and global trace, use the **clear platform hardware chassis active qfp feature wireless trace-buffer punt-inject** command.

clear platform hardware chassis active qfp feature wireless trace-buffer punt-inject { **all** | **conditions** | **filtered-trace** | **global-trace** }

Syntax Description

all	Clears conditions, global trace buffer, and filtered-trace buffer.
conditions	Clears all filtered-trace conditions.
filtered-trace	Clears filtered trace buffer.
global-trace	Clears global trace buffer.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.6.1	This command was introduced.

Example

The following example shows you how to clear QFP wireless punt inject packet filtered trace:

```
Device# clear platform hardware chassis active qfp feature wireless punt-inject all
```

clear platform software rif-mgr chassis active R0 clear-lmp-counters

To clear the control message statistics in an active instance, use the **clear platform software rif-mgr chassis active R0 clear-lmp-counters** command.

clear platform software rif-mgr chassis active R0 clear-lmp-counters

Syntax Description

rif-mgr	Displays information about the RIF manager.
chassis	Displays information about the chassis.
active	Specifies the Active instance.
R0	Specifies the Route-Processor slot 0.
clear-lmp-counters	Clears the LMP statistics.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.6.1	This command was introduced.

Example

The following example shows how to clear the control message statistics in an active instance:

```
Device# clear platform software rif-mgr chassis active R0 clear-lmp-counters
```

clear platform software rif-mgr chassis standby R0 clear-lmp-counters

To clear the control message statistics in a standby instance, use the **clear platform software rif-mgr chassis standby R0 clear-lmp-counters** command.

clear platform software rif-mgr chassis standby R0 clear-lmp-counters

Syntax Description

rif-mgr	Displays information about the RIF manager.
chassis	Displays information about the chassis.
standby	Specifies the Standby instance.
R0	Specifies the Route-Processor slot 0.
clear-lmp-counters	Clears the LMP statistics.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.6.1	This command was introduced.

Example

The following example shows how to clear the control message statistics in a standby instance:

```
Device# clear platform software rif-mgr chassis standby R0 clear-lmp-counters
```

clear radius statistics

To clear the radius server information statistics, use the **clear radius statistics** command.

clear radius statistics

Syntax Description

There are no arguments for this command.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Example

The following example shows how to clear the radius server information statistics:

```
Device# clear radius statistics
```

clear subscriber policy peer

To clear the display of the details of a subscriber policy peer connection, use the **clear subscriber policy peer**command in privileged EXEC mode.

clear subscriber policy peer {**address** *ip-address* | **handle** *connection-handle-id* | **session** | **all**}

Syntax Description

address	Clears the display of a specific peer connection, identified by its IP address.
ip-address	IP address of the peer connection to be cleared.
handle	Clears the display of a specific peer connection, identified by its handle.
connection-handle-id	Handle ID for the peer connection handle.
session	Clears the display of sessions with the given peer.
all	Clears the display of all peer connections.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB

Usage Guidelines

The **clear subscriber policy peer** command ends the peering relationship between the Intelligent Services Gateway (ISG) device and selected Service Control Engine (SCE) devices. However, the SCE will attempt to reconnect with the ISG device after a configured amount of time. The **clear subscriber policy peer** command can remove select session associations from a particular SCE device.

Examples

The following example shows how the **clear subscriber policy peer**command is used at the router prompt to clear the display of all details of the subscriber policy peer connection.

```
Router# clear subscriber policy peer all
```

Related Commands

Command	Description
show subscriber-policy peer	Displays the details of a subscriber policy peer.
subscriber-policy	Defines or modifies the forward and filter decisions of the subscriber policy.

clear wireless stats mobility

To clear the event and message level statistics, use the **clear wireless stats mobility** command.

clear wireless stats mobility

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Usage Guidelines

This example shows how to clear the event and message level statistics:

```
Device# clear wireless stats mobility
```

clear wireless stats mobility peer ip

To clear the control and data link flap counters associated with a peer, use the **clear wireless stats mobility peer ip** command.

clear wireless stats mobility peer ip *ip-address*

Syntax Description

ip-address	IP address of the remote peer.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Usage Guidelines

This example shows how to clear the control and data link flap counters associated with a peer:

```
Device# clear wireless stats mobility peer ip 192.0.2.51
```

clear wireless wps rogue ap

To clear all rogue APs or rogue APs with specific MAC addresses, use the **clear wireless wps rogue ap** command.

clear wireless wps rogue ap { **all** | **mac-address** <*MAC Address*> }

Syntax Description

all	Clears all the rogue APs.
mac-address <*MAC Address*>	Clears the rogue APs with specific MAC addresses.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Amsterdam 16.12.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows you how to clear all rogue APs or rogue APs with specific MAC addresses:

```
Device# clear wireless wps rogue ap all
Device# clear wireless wps rogue ap mac-address 10.10.1
```

clear wireless wps rogue client

To clear all rogue clients or client with specific MAC addresses, use the **clear wireless wps rogue client** command.

clear wireless wps rogue client { **all** | **mac-address** <*MAC Address*> }

Syntax Description

all	Clears all the rogue clients.
mac-address <*MAC Address*>	Clears the rogue clients with specific MAC addresses.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Amsterdam 16.12.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows you how to clear all rogue clients or rogue clients with specific MAC addresses:

```
Device# clear wireless wps rogue client all
Device# clear wireless wps rogue client mac-address 10.10.1
```

clear wireless wps rogue stats

To clear rogue statistics, use the **clear wireless wps rogue stats** command.

clear wireless wps rogue stats

Syntax Description

This command has no arguments.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Amsterdam 16.12.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows you how to clear rogue statistics:

```
Device# clear wireless wps rogue stats
```

clear wlan sort statistics

To clear the sorted WLAN statistics, use the **clear wlan sort statistics** command.

clear wlan sort statistics

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.1.1s	This command was introduced.

This example shows how to clear the sorted WLAN statistics:

```
Device# clear wlan sort statistics
```

client-access (mesh)

To configure backhaul with client access AP for a mesh AP profile, use the **client-access** command.

client-access

Syntax Description

This command has no keywords or arguments.

Command Default

Backhaul client access is disabled.

Command Modes

config-wireless-mesh-profile

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Example

The following example shows how to configure backhaul with client access AP for a mesh AP profile:

```
Device # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device (config)# wireless profile mesh mesh-profile
Device (config-wireless-mesh-profile)# client-access
```

client association limit

To configure the maximum number of client connections on a WLAN, use the **client association limit** command. To disable clients association limit on the WLAN, use the **no** form of this command.

client association limit {*association-limit*}
no client association limit {*association-limit*}

Syntax Description

association-limit	Number of client connections to be accepted. The range is from 0 to . A value of zero (0) indicates no set limit.

Command Default

The maximum number of client connections is set to 0 (no limit).

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

This example shows how to configure a client association limit on a WLAN and configure the client limit to 200:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# shutdown
Device(config-wlan)# client association limit 200
Device(config-wlan)# no shutdown
Device(config-wlan)# end
```

This example shows how to disable a client association limit on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# shutdown
Device(config-wlan)# no client association limit
Device(config-wlan)# no shutdown
Device(config-wlan)# end
```

This example shows how to configure a client association limit per radio on a WLAN and configure the client limit to 200:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# client association limit radio 200
Device(config-wlan)# no shutdown
Device(config-wlan)# end
```

This example shows how to configure a client association limit per AP on a WLAN and configure the client limit to 300::

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# client association limit ap 300
Device(config-wlan)# no shutdown
Device(config-wlan)# end
```

client-aware-fra

To configure the client aware Flexible Radio Assignment (FRA) , use the **client-aware-fra** {**client-count-reset** *client-count* | **client-reset-util** *util-percentage*} command in the RF profile configuration mode.

Use the no form of the **client-reset-util** command to disable the feature.

client-aware-fra { **client-count-reset** *client-count* | **client-reset-util** *util-percentage* }

no client-aware-fra client-reset-util *util-percentage*

Syntax Description

client-count-reset	Configures the client count threshold for radio to switch from 6-GHz to 5-GHz.
client-count	Specifies the 6-GHz client count. The value range is from 1 and 10 clients.
client-reset-util	Configures the utilization threshold for radio to switch from 6-GHz to 5-GHz.
util-percentage	Specifies the utilization percentage. The value range is from 0 to 100 percent.

Command Default

None

Command Modes

RF Profile Configuration

Command History

Release	Modification
Cisco IOS XE Cupertino 17.9.1	This command was introduced.

Example

This example shows how to configure the client aware Flexible Radio Assignment (FRA):

```
Device(config)# ap dot11 6ghz rf-profile rf-profile-name
Device(conf-rf-profile)# client-aware-fra client-count-reset 1
Device(conf-rf-profile)# client-aware-fra client-reset-util 5
```

cloud-services aws s3 profile

To configure Amazon S3 cloud services profile, use the **cloud-services aws s3 profile** command. To remove Amazon S3 cloud services profile, use the **no** form of the command.

cloud-services aws s3 profile *profile-name*

no cloud-services aws s3 profile *profile-name*

Syntax Description

profile-name	Amazon S3 cloud services profile name.

Command Default

Profile is not configured.

Command Modes

S3fs Profile Configuration (config-s3fs-profile)

Command History

Release	Modification
Cisco IOS XE 17.13.1	This command was introduced.

Usage Guidelines

Use only alphanumeric characters for the profile name. Underscore (_) is the only special character that is supported.

Examples

The following example shows how to configure Amazon S3 cloud services profile.

```
Device# configure terminal
Device(config)# cloud-services aws s3 profile 9800_XT_HD
```

cloud-services aws cloudwatch profile

To configure AWS CloudWatch profile, use the **cloud-services aws cloudwatch profile** command. To remove AWS CloudWatch profile, use the **no** form of the command.

cloud-services aws cloudwatch profile *profile-name*

no cloud-services aws cloudwatch profile *profile-name*

Syntax Description

profile-name	AWS CloudWatch profile name.

Command Default

Profile is not configured.

Command Modes

CloudWatch Profile Configuration (config-cloudwatch-profile)

Command History

Release	Modification
Cisco IOS XE 17.13.1	This command was introduced.

Usage Guidelines

When the profile is disabled, all the associated configurations are also disabled and syslog messages are not sent to the AWS CloudWatch service.

Examples

The following example shows how to configure AWS CloudWatch profile.

```
Device# configure terminal
Device(config)# cloud-services aws cloudwatch profile test_profile
```

channel foreign

To configure the RF Profile DCA foreign AP contribution, use the **channel foreign** command. To disable the DCA Foreign AP Contribution, use the **no** form of this command.

channel foreign

Syntax Description

foreign	Configures the RF Profile DCA foreign AP contribution.

Command Default

None

Command Modes

config-rf-profile

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines

None

This example shows how to configure the RF profile DCA foreign AP contribution.

```
Device(config-rf-profile)#channel foreign
```

channel chan-width

To configure the RF profile DCA channel width, use the **channel chan-width** command.

channel chan-width {**160** | **20** | **40** | **80** | **80+80** | **best**}

Syntax Description

160	160 MHz.
20	20 MHz.
40	40 MHz.
80	80 MHz.
80+80	80+80 MHz.
best	Best channel width.

Command Default

None

Command Modes

RF Profile Configuration (config-rf-profile)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

Example

The following example shows how to configure the RF profile DCA channel width.

```
Device(config-rf-profile)# channel chan-width 160
```

channel psc

To enable or disable the preferred scanning channel (PSC) bias for DCA, use the **channel psc** command, in the RF configuration mode. Use the **no** form of this command to disable this feature.

channel psc

no channel psc

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

RF configuration mode

Command History

Release	Modification
Cisco IOS XE Cupertino 17.7.1	This command was introduced.

Example

The following example shows how to enable or disable the preferred scanning channel (PSC) bias for DCA:

```
Device(config)# ap dot11 6ghz rf-profile rf-profile-name
Device(config-rf-profile)# channel psc
```

client-l2-vnid

To configure the client l2-vnid on a wireless fabric profile, use the **client-l2-vnid** command.

client-l2-vnid *vnid*

Syntax Description

vnid	Configures client l2-vnid. Valid range is 0 to 16777215.

Command Default

None

Command Modes

config-wireless-fabric

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure the client l2-vnid value on a wireless fabirc profile:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile fabric fabric-profile-name
Device(config-wireless-fabric)# client-l2-vnid 10
```

client-steering

To configure 6-GHz client steering on the WLAN, use the **client-steering** command. Use the **no** form of this command to disable this feature.

client-steering

no client-steering

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

WLAN configuration mode

Command History

Release	Modification
Cisco IOS XE Cupertino 17.7.1	This command was introduced.

Example

This example shows how to configure 6-GHz client steering on WLAN:

```
Device # configure terminal
Device (config)# wlan wlan-name 18 ssid-name
Device (config-wlan)# client-steering
```

collect counter

To configure the number of bytes or packets in a flow as a non-key field for a flow record, use the **collect counter** command in flow record configuration mode. To disable the use of the number of bytes or packets in a flow (counters) as a non-key field for a flow record, use the **no** form of this command.

Command Default

The number of bytes or packets in a flow is not configured as a non-key field.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

To return this command to its default settings, use the **no collect counter** or **default collect counter** flow record configuration command.

The following example configures the total number of bytes in the flows as a non-key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)#collect counter bytes long
```

The following example configures the total number of packets from the flows as a non-key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect counter packets long
```

collect wireless ap mac address (wireless)

To enable the collection of MAC addresses of the access points that the wireless client is associated with, use the **collect wireless ap mac address** command in the flow record configuration mode. To disable the collection of access point MAC addresses, use the **no** form of this command.

collect wireless ap mac address
no collect wirelessap mac address

Syntax Description

This command has no arguments or keywords.

Command Default

The collection of access point MAC addresses is not enabled by default.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

The Flexible NetFlow **collect** commands are used to configure non-key fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in non-key fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a non-key field does not create a new flow. In most cases, the values for non-key fields are taken from only the first packet in the flow.

The following example configures the flow record to enable the collection of MAC addresses of the access points that the wireless client is associated with:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect wireless ap mac address
```

collect wireless client mac address (wireless)

To enable the collection of MAC addresses of the wireless clients that the access point is associated with, use the **collect wireless client mac address** command in the flow record configuration mode. To disable the collection of access point MAC addresses, use the **no** form of this command.

collect wirelessclient mac address
no collect wireless client mac address

Syntax Description

This command has no arguments or keywords.

Command Default

The collection of wireless client MAC addresses is not enabled by default.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

The Flexible NetFlow **collect** commands are used to configure non-key fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in non-key fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a non-key field does not create a new flow. In most cases, the values for non-key fields are taken from only the first packet in the flow.

The following example configures the flow record to enable the collection of MAC addresses of the access points that the wireless client is associated with:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect wireless client mac address
```

condition chan-width

To configure channel width and band for rogue detection, use the **condition chan-width** command. To remove channel width and band from rogue detection, use the **no** form of this command.

condition chan-width { **160MHz** | **20MHz** | **40MHz** | **80MHz** } **band** { **2.4GHz** | **5GHz** | **6GHz** }

no condition chan-width

Syntax Description

160MHz	Specifies channel width as 160 MHz.
20MHz	Specifies channel width as 20 MHz.
40MHz	Specifies channel width as 40 MHz.
80MHz	Specifies channel width as 80 MHz.
band	Specifies the radio band.
2.4GHz	Specifies the radio band as 2.4 GHz.
5GHz	Specifies the radio band as 5 GHz.
6GHz	Specifies the radio band as 6 GHz.

Command Default

Channel width is not configured.

Command Modes

Rule configuration (config-rule)

Command History

Release	Modification
Cisco IOS XE Dublin 17.12.1	This command was introduced.

Usage Guidelines

If the classification is **Friendly**, the value configured is the minimum channel width.

If the classification is **Custom**, **Malicious**, or **Delete**, the value configured is the maximum channel width.

Examples

The following example shows how to configure channel width value and band for rogue-detection classification:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless wps rogue rule 1 priority 1
Device(config-rule)#condition chan-width 20MHz band 5gHz
```

connection-capability

To configure a Hotspot 2.0 connection capability, use the **connection-capability** command. To remove the Hotspot 2.0 connection capability, use the **no** form of the command.

connection-capability *ip-protocol port-number* {**closed** | **open** | **unknown**}

Syntax Description

ip-protocol	IP number. Valid range is from 0-255.
port-number	Port number. Valid range is from 0-65535.
closed	Indicates that connection is closed mode.
open	Indicates that connection is open mode.
unknown	Indicates that connection status is unknown.

Command Default

None

Command Modes

Wireless ANQP Server Configuration (config-wireless-anqp-server)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

The following table lists the pre-defined open ports and protocols.

Table 5: Open Ports and Protocols

IP Protocol	Port Number	Description
1	0	ICMP. Used for diagnostics.
6	20	FTP
6	22	SSH
6	80	HTTP
6	443	Used by HTTPS and TLS VPNs.
6	1723	Used by Point to Point Tunneling Protocol VPNs.
6	5060	VoIP
17	500	Used by IKEv2 (IPsec VPN).
17	5060	VoIP
17	4500	May be used by IKEv2 (IPsec VPN).

IP Protocol	Port Number	Description
50	0	ESP. Used by IPsec VPNs.

Example

The following example shows how to configure Hotspot 2.0 connection capability:

```
Device(config)#wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# connection-capability 12 655 open
```

consent activation-mode merge

To enable the policy activation mode and merge it with the policy applied for 802.1X or MAC Authentication Bypass (MAB), thereby enabling a client to access the network, use the **consent activation-mode merge** command in the parameter map configuration mode. To disable this feature, use the **no** form of this command.

consent activation-mode merge

no consent activation-mode merge

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Parameter map configuration mode

Command History

Release	Modification
Cisco IOS XE Dublin 17.11.1	This command was introduced.

Examples

The following example shows how to enable the policy activation mode and merge it with the policy applied for 802.1X or MAC Authentication Bypass (MAB), thereby enabling a client to access the network:

```
Device# configure terminal
Device(config)# parameter-map type webauth parameter-map-name
Device(config-params-parameter-map)# consent activation-mode merge
```

console

To enable an AP serial console port, use the **console** command in the AP profile configuration. Use the **no** form of this command to disable the feature.

console

no console

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

AP Profile Configuration

Command History

Release	Modification
Cisco IOS XE Cupertino 17.9.1	This command was introduced.

Example

This example shows how to enable an AP serial console port:

```
Device(config)# ap profile ap-profile-name
Device(config-ap-profile)# console
```

console speed

To configure the console speed for APs, use the **console speed** command in the AP profile configuration. Use the **none** form of the command to maintain the current configuration and retain the AP's console speed.

console speed { **9600** | **115200** | **none** }

Syntax Description

9600	Sets the AP console speed to 9600 bps.
115200	Sets the AP console speed to 115200 bps.
none	Sets no console speed.

Command Default

No console speed

Command Modes

AP profile configuration

Command History

Release	Modification
Cisco IOS XE 26.1.1	This command was introduced.

Example

This example shows how to enable the serial console speed for APs:

```
Device(config)# ap profile ap-profile-name
Device(config-ap-profile)# console speed
```

controller

To enter SD service controller connectivity parameter configuration mode, use the **controller** command. To exit SD service controller configuration mode, use the **exit** command.

controller

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

SD Service Configuration (config-sd-service)

Command History

Release	Modification
Cisco IOS XE Cupertino 17.7.1	This command was introduced.

Examples

The following example shows how to enable SD service controller connectivity parameter configuration mode:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# avc sd-service
Device(config-sd-service)# controller
```

convergence

To configure mesh convergence method, use the **convergence** command.

convergence { **fast** | **noise-tolerant-fast** | **standard** | **very-fast** }

Syntax Description

fast	Configures fast convergence method.
noise-tolerant-fast	Configures noise-tolerant fast convergence method method to handle unstable RF environment.
standard	Configures standard convergence method.
very-fast	Configures very fast convergence method.

Command Default

Standard

Command Modes

config-wireless-mesh-profile

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure the fast convergence method for a mesh AP profile:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile mesh mesh-profile
Device(config-wireless-mesh-profile)# convergence fast
```

copy configuration download

To download a workgroup bridge (WGB) configuration file from the SFTP or TFTP server, use the **copy configuration download** command.

copy configuration download { **sftp:** | **tftp:** } *ip-address* [*directory*] [*file-name*]

Syntax Description

sftp:	Selects SFTP server.
tftp:	Selects TFTP server.
ip-address	IP address of the SFTP or TFTP server that you want to use.
directory	(Optional) Directory name to use in the SFTP or TFTP server.
file-name	(Optional) WGB configuration file name.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Cupertino 17.8.1	This command was introduced.

Usage Guidelines

You can enter this command on the AP console only if the AP is in the WGB mode.

Examples

The following example shows how to select a WGB configuration file from the SFTP server:

```
Device# copy configuration download sftp: 10.10.10.1 C:sample.txt
```

copy configuration upload

To create a workgroup bridge (WGB) configuration file and upload it to the SFTP or TFTP server, use the **copy configuration upload** command.

copy configuration upload { **sftp:** | **tftp:** } *ip-address* [*directory*] [*file-name*]

Syntax Description

sftp:	Selects SFTP server.
tftp:	Selects TFTP server.
ip-address	IP address of the SFTP or TFTP server that you want to use.
directory	(Optional) Directory name to use in the SFTP or TFTP server.
file-name	(Optional) WGB configuration file name.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Cupertino 17.8.1	This command was introduced.

Usage Guidelines

You can enter this command on the AP console only if the AP is in the WGB mode.

Examples

The following example shows how to create a WGB configuration file and upload it to the SFTP server:

```
Device# copy configuration upload sftp: 10.10.10.1 C:sample.txt
```

core-dump kernel limit

To limit the number of kernel core dumps collected on an AP, use the **core-dump kernel limit** command. To disable this feature, use the **no** form of this command.

core-dump kernel limit *limit*

no core-dump kernel limit

Syntax Description

limit	The maximum number of kernel core dumps to be collected on an AP. Valid range is from 0 to 5. The default value is 0.

Command Default

None

Command Modes

AP profile configuration (config-ap-profile)

Command History

Release	Modification
Cisco IOS XE Dublin 17.12.1	This command was introduced.

Usage Guidelines

Every connected AP reboots after enabling or disabling the **core-dump kernel limit** command.

Examples

The following example shows how to limit the number of kernel core dumps collected on an AP:

```
Device(config)# ap profile default-ap profile
Device(config-ap-profile)# core-dump kernel limit 3
```

core-dump kernel type

To configure the type of kernel core dump to be collected on the AP, use the **core-dump kernel type** command. To disable kernel core dump collection, use the **disable** option of this command.

core-dump kernel type { **disable** | **full-dump** | **mini-dump** }

Syntax Description

disable	Disables kernel core dump collection
full-dump	Enables full kernel core dump mode
mini-dump	Enables mini kernel core dump mode

Command Default

None

Command Modes

AP profile configuration (config-ap-profile)

Command History

Release	Modification
Cisco IOS XE 17.14.1	This command was introduced.

Usage Guidelines

Changing the kernel core dump type from disabled to full-dump or mini-dump or vice versa will cause the APs to reboot.

Examples

The following example shows how to configure the type of kernel core dump to be collected on the AP.

```
Device# configure terminal
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# core-dump kernel type mini-dump
```

coverage

To configure the voice and data coverage, use the **coverage** command. To reset the minimum RSSI value use the **no** form of this command.

coverage {**data** | **voice**} **rssi threshold** *value*

Syntax Description

data	Configure Coverage Hole Detection for data packets.
voice	Configure Coverage Hole Detection for voice packets.
value	Minimum RSSI value for the packets received by the access point. The valid rage is between –90 and –60 dBm.

Command Default

None

Command Modes

config-rf-profile

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines

None

This example shows how to configure the coverage hole detection for data packets.

```
Device(config-rf-profile)#coverage data rssi threshold -85
```

crypto key generate rsa

To generate Rivest, Shamir, and Adelman (RSA) key pairs, use the **crypto key generate rsa** commandinglobal configuration mode.

crypto key generate rsa [**general-keys** | **usage-keys** | **signature** | **encryption**] [**label** *key-label*] [**exportable**] [**modulus** *modulus-size*] [**storage** *devicename* **:**] [**redundancy**] [**on** *devicename* **:**]

Syntax Description

general-keys	(Optional) Specifies that a general-purpose key pair will be generated, which is the default.
usage-keys	(Optional) Specifies that two RSA special-usage key pairs, one encryption pair and one signature pair, will be generated.
signature	(Optional) Specifies that the RSA public key generated will be a signature special usage key.
encryption	(Optional) Specifies that the RSA public key generated will be an encryption special usage key.
label *key-label*	(Optional) Specifies the name that is used for an RSA key pair when they are being exported. If a key label is not specified, the fully qualified domain name (FQDN) of the router is used.
exportable	(Optional) Specifies that the RSA key pair can be exported to another Cisco device, such as a router.
modulus *modulus-size*	(Optional) Specifies the IP size of the key modulus. By default, the modulus of a certification authority (CA) key is 1024 bits. The recommended modulus for a CA key is 2048 bits. The range of a CA key modulus is from 350 to 4096 bits. **Note** Effective with Cisco IOS XE Release 2.4 and Cisco IOS Release 15.1(1)T, the maximum key size was expanded to 4096 bits for private key operations. The maximum for private key operations prior to these releases was 2048 bits.
storage *devicename* **:**	(Optional) Specifies the key storage location. The name of the storage device is followed by a colon (:).
redundancy	(Optional) Specifies that the key should be synchronized to the standby CA.
on *devicename* **:**	(Optional) Specifies that the RSA key pair will be created on the specified device, including a Universal Serial Bus (USB) token, local disk, or NVRAM. The name of the device is followed by a colon (:). Keys created on a USB token must be 2048 bits or less.

Command Default

RSA key pairs do not exist.

Command Modes

Global configuration (config)

From Cisco IOS XE Release 17.11.1a, the command mode is Privileged EXEC (#)

Command History

Release	Modification
11.3	This command was introduced.
12.2(8)T	The *key-label* argumentwas added.
12.2(15)T	The **exportable** keyword was added.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.4(4)T	The **storage** keyword and *devicename* **:** argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	The **storage** keyword and *devicename* **:** argument were implemented on the Cisco 7200VXR NPE-G2 platform. The **signature**, **encryption** and **on** keywords and *devicename* **:** argument were added.
12.4(24)T	Support for IPv6 Secure Neighbor Discovery (SeND) was added.
XE 2.4	The maximum RSA key size was expanded from 2048 to 4096 bits for private key operations.
15.0(1)M	This command was modified. The **redundancy** keyword was introduced.
15.1(1)T	This command was modified. The range value for the **modulus** keyword value is extended from 360 to 2048 bits to 360 to 4096 bits.
15.2(2)SA2	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.
Cisco IOS XE Release 17.11.1a	The default command mode for this command has changed from Global configuration (config) to Privileged EXEC (#).

Usage Guidelines

Note Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

Use this command to generate RSA key pairs for your Cisco device (such as a router).

RSA keys are generated in pairs--one public RSA key and one private RSA key.

If your router already has RSA keys when you issue this command, you will be warned and prompted to replace the existing keys with new keys.

Note Before issuing this command, ensure that your router has a hostname and IP domain name configured (with the **hostname** and **ip domain-name** commands). You will be unable to complete the **crypto key generate rsa** command without a hostname and IP domain name. (This situation is not true when you generate only a named key pair.)

Note Secure Shell (SSH) may generate an additional RSA key pair if you generate a key pair on a router having no RSA keys. The additional key pair is used only by SSH and will have a name such as {*router_FQDN* }.server. For example, if a router name is "router1.cisco.com," the key name is "router1.cisco.com.server."

This command is not saved in the router configuration; however, the RSA keys generated by this command are saved in the private configuration in NVRAM (which is never displayed to the user or backed up to another device) the next time the configuration is written to NVRAM.

Note If the configuration is not saved to NVRAM, the generated keys are lost on the next reload of the router.

There are two mutually exclusive types of RSA key pairs: special-usage keys and general-purpose keys. When you generate RSA key pairs, you will be prompted to select either special-usage keys or general-purpose keys.

Special-Usage Keys

If you generate special-usage keys, two pairs of RSA keys will be generated. One pair will be used with any Internet Key Exchange (IKE) policy that specifies RSA signatures as the authentication method, and the other pair will be used with any IKE policy that specifies RSA encrypted keys as the authentication method.

A CA is used only with IKE policies specifying RSA signatures, not with IKE policies specifying RSA-encrypted nonces. (However, you could specify more than one IKE policy and have RSA signatures specified in one policy and RSA-encrypted nonces in another policy.)

If you plan to have both types of RSA authentication methods in your IKE policies, you may prefer to generate special-usage keys. With special-usage keys, each key is not unnecessarily exposed. (Without special-usage keys, one key is used for both authentication methods, increasing the exposure of that key.)

General-Purpose Keys

If you generate general-purpose keys, only one pair of RSA keys will be generated. This pair will be used with IKE policies specifying either RSA signatures or RSA encrypted keys. Therefore, a general-purpose key pair might get used more frequently than a special-usage key pair.

Named Key Pairs

If you generate a named key pair using the *key-label*argument, you must also specify the **usage-keys** keyword or the **general-keys** keyword. Named key pairs allow you to have multiple RSA key pairs, enabling the Cisco IOS software to maintain a different key pair for each identity certificate.

Modulus Length

When you generate RSA keys, you will be prompted to enter a modulus length. The longer the modulus, the stronger the security. However a longer modules takes longer to generate (see the table below for sample times) and takes longer to use.

Table 6: Sample Times by Modulus Length to Generate RSA Keys

Router	360 bits	512 bits	1024 bits	2048 bits (maximum)
Cisco 2500	11 seconds	20 seconds	4 minutes, 38 seconds	More than 1 hour
Cisco 4700	Less than 1 second	1 second	4 seconds	50 seconds

Cisco IOS software does not support a modulus greater than 4096 bits. A length of less than 512 bits is normally not recommended. In certain situations, the shorter modulus may not function properly with IKE, so we recommend using a minimum modulus of 2048 bits.

Note As of Cisco IOS Release 12.4(11)T, peer *public* RSA key modulus values up to 4096 bits are automatically supported. The largest private RSA key modulus is 4096 bits. Therefore, the largest RSA private key a router may generate or import is 4096 bits. However, RFC 2409 restricts the private key size to 2048 bits or less for RSA encryption. The recommended modulus for a CA is 2048 bits; the recommended modulus for a client is 2048 bits.

Additional limitations may apply when RSA keys are generated by cryptographic hardware. For example, when RSA keys are generated by the Cisco VPN Services Port Adapter (VSPA), the RSA key modulus must be a minimum of 384 bits and must be a multiple of 64.

Specifying a Storage Location for RSA Keys

When you issue the **crypto key generate rsa** command with the **storage** *devicename* **:** keyword and argument, the RSA keys will be stored on the specified device. This location will supersede any **crypto key storage** command settings.

Specifying a Device for RSA Key Generation

As of Cisco IOS Release 12.4(11)T and later releases, you may specify the device where RSA keys are generated. Devices supported include NVRAM, local disks, and USB tokens. If your router has a USB token configured and available, the USB token can be used as cryptographic device in addition to a storage device. Using a USB token as a cryptographic device allows RSA operations such as key generation, signing, and authentication of credentials to be performed on the token. The private key never leaves the USB token and is not exportable. The public key is exportable.

RSA keys may be generated on a configured and available USB token, by the use of the **on** *devicename* **:** keyword and argument. Keys that reside on a USB token are saved to persistent token storage when they are generated. The number of keys that can be generated on a USB token is limited by the space available. If you attempt to generate keys on a USB token and it is full you will receive the following message:

```
% Error in generating keys:no available resources
```

Key deletion will remove the keys stored on the token from persistent storage immediately. (Keys that do not reside on a token are saved to or deleted from nontoken storage locations when the **copy**or similar command is issued.)

For information on configuring a USB token, see " Storing PKI Credentials " chapter in the Cisco IOS Security Configuration Guide, Release 12.4T. For information on using on-token RSA credentials, see the " Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment " chapter in the Cisco IOS Security Configuration Guide , Release 12.4T.

Specifying RSA Key Redundancy Generation on a Device

You can specify redundancy for existing keys only if they are exportable.

Examples

The following example generates a general-usage 1024-bit RSA key pair on a USB token with the label “ms2” with crypto engine debugging messages shown:

```
Router(config)# crypto key generate rsa label ms2 modulus 2048 on usbtoken0:
The name for the keys will be: ms2
% The key modulus size is 2048 bits
% Generating 1024 bit RSA keys, keys will be on-token, non-exportable...
Jan 7 02:41:40.895: crypto_engine: Generate public/private keypair [OK]
Jan 7 02:44:09.623: crypto_engine: Create signature
Jan 7 02:44:10.467: crypto_engine: Verify signature
Jan 7 02:44:10.467: CryptoEngine0: CRYPTO_ISA_RSA_CREATE_PUBKEY(hw)(ipsec)
Jan 7 02:44:10.467: CryptoEngine0: CRYPTO_ISA_RSA_PUB_DECRYPT(hw)(ipsec)
```

Now, the on-token keys labeled “ms2” may be used for enrollment.

The following example generates special-usage RSA keys:

```
Router(config)# crypto key generate rsa usage-keys
The name for the keys will be: myrouter.example.com
Choose the size of the key modulus in the range of 360 to 2048 for your Signature Keys.
Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus[512]? <return>
Generating RSA keys.... [OK].
Choose the size of the key modulus in the range of 360 to 2048 for your Encryption Keys.
Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus[512]? <return>
Generating RSA keys.... [OK].
```

The following example generates general-purpose RSA keys:



Note You cannot generate both special-usage and general-purpose keys; you can generate only one or the other.

```
Router(config)# crypto key generate rsa general-keys
The name for the keys will be: myrouter.example.com
Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose
Keys. Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus[512]? <return>
Generating RSA keys.... [OK].
```

The following example generates the general-purpose RSA key pair “exampleCAkeys”:

```
crypto key generate rsa general-keys label exampleCAkeys
crypto ca trustpoint exampleCAkeys
 enroll url
http://exampleCAkeys/certsrv/mscep/mscep.dll
 rsakeypair exampleCAkeys 1024 1024
```

The following example specifies the RSA key storage location of “usbtoken0:” for “tokenkey1”:

crypto key generate rsa general-keys label tokenkey1 storage usbtoken0:

The following example specifies the **redundancy** keyword:

```
Router(config)# crypto key generate rsa label MYKEYS redundancy
The name for the keys will be: MYKEYS
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]:
% Generating 512 bit RSA keys, keys will be non-exportable with redundancy...[OK]
```

Related Commands

Command	Description
copy	Copies any file from a source to a destination, use the copy command in privileged EXEC mode.
crypto key storage	Sets the default storage location for RSA key pairs.
debug crypto engine	Displays debug messages about crypto engines.
hostname	Specifies or modifies the hostname for the network server.
ip domain-name	Defines a default domain name to complete unqualified hostnames (names without a dotted-decimal domain name).
show crypto key mypubkey rsa	Displays the RSA public keys of your router.
show crypto pki certificates	Displays information about your PKI certificate, certification authority, and any registration authority certificates.

crypto pki trustpoint

To create a new TrustPoint dedicated for a single CA certificate, use the **crypto pki trustpoint** command.

crypto pki trustpoint

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global Configuration

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.5.1	This command was introduced.

Usage Guidelines

This example shows how to create a new TrustPoint dedicated for a single CA certificate:

```
Device# configure terminal
Device(config)# crypto pki trustpoint <tp_name>
Device(ca-trustpoint)# enrollment terminal
Device(ca-trustpoint)# exit
Device(config)# crypto pki authenticate <tp_name>
<<< PASTE CA-CERT in PEM format followed by quit >>>
```

crypto pki trust pool import terminal

To import the root certificate by pasting the CA certificate from the **digicert.com**, use the **crypto pki trust pool import terminal** command.

crypto pki trust pool import terminal

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global Configuration

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.5.1	This command was introduced.

Usage Guidelines

This example shows how to import the root certificate by pasting the CA certificate from the **digicert.com**:

```
Device# configure terminal
Device(config)# crypto pki trust pool import terminal
Device(config)# end
```

crypto pki trustpool clean

To erase the downloaded CA certificate bundles, use the **crypto pki trustpool clean** command.

crypto pki trustpool clean

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global Configuration

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.5.1	This command was introduced.

Usage Guidelines

This example shows how to erase the downloaded CA certificate bundles:

```
Device# configure terminal
Device(config)# crypto pki trustpool clean
Device(config)# end
```

cts inline-tagging

To configure Cisco TrustSec (CTS) inline tagging, use the **cts inline-tagging** command.

cts inline-tagging

Syntax Description

This command has no keywords or arguments.

Command Default

Inline tagging is not configured.

Command Modes

wireless policy configuration (config-wireless-policy)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Example

This example shows how to configure CTS inline tagging.

```
Device(config-wireless-policy)# cts inline-tagging
```

cts role-based enforcement

To configure Cisco TrustSec (CTS) SGACL enforcement, use the **cts role-based enforcement** command.

cts role-based enforcement

Syntax Description

This command has no keywords or arguments.

Command Default

SGACL is not enforced.

Command Modes

wireless policy configuration (config-wireless-policy)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Example

This example shows how to configure CTS SGACL enforcement.

```
Device(config-wireless-policy)# cts role-based enforcement
```

cts sgt

To set the Cisco TrustSec (CTS) default security group tag (SGT), use the **cts sgt** command.

cts sgt *sgt-value*

Syntax Description

sgt-value	Security group tag value.

Command Default

SGT tag is not set.

Command Modes

wireless policy configuration (config-wireless-policy)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Example

This example shows how to set the default SGT.

```
Device(config-wireless-policy)# cts sgt 100
```

custom-page login device

To configure a customized login page, use the **custom-page login device** command.

custom-page login device *html-filename*

Syntax Description

html-filename	Enter the HTML filename of the login page.

Command Default

None

Command Modes

config-params-parameter-map

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure a customized login page:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# parameter-map type webauth parameter-map-name
Device(config-params-parameter-map)# custom-page login device bootflash:login.html
```

default

To set the parameters to their default values, use the **default** command.

default {**aaa-override** | **accounting-list** | **band-select** | **broadcast-ssid** | **call-snoop** | **ccx** | **channel-scan** | **parameters** | **chd** | **client** | **datalink** | **diag-channel** | **dtim** | **exclusionlist** | **ip** | **ipv6** | **load-balance** | **local-auth** | **mac-filtering** | **media-stream** | **mfp** | **mobility** | **nac** | **passive-client** | **peer-blocking** | **radio** | **roamed-voice-client** | **security** | **service-policy** | **session-timeout** | **shutdown** | **sip-cac** | **static-ip** | **uapsd** | **wgb** | **wmm**}

Syntax Description

aaa-override	Sets the AAA override parameter to its default value.
accounting-list	Sets the accounting parameter and its attributes to their default values.
band-select	Sets the band selection parameter to its default values.
broadcast-ssid	Sets the broadcast Service Set Identifier (SSID) parameter to its default value.
call-snoop	Sets the call snoop parameter to its default value.
ccx	Sets the Cisco client extension (Cisco Aironet IE) parameters and attributes to their default values.
channel-scan	Sets the channel scan parameters and attributes to their default values.
chd	Sets the coverage hold detection parameter to its default value.
client	Sets the client parameters and attributes to their default values.
datalink	Sets the datalink parameters and attributes to their default values.
diag-channel	Sets the diagnostic channel parameters and attributes to their default values.
dtim	Sets the Delivery Traffic Indicator Message (DTIM) parameter to its default value.
exclusionlist	Sets the client exclusion timeout parameter to its default value.
ip	Sets the IP parameters to their default values.
ipv6	Sets the IPv6 parameters and attributes to their default values.
load-balance	Sets the load-balancing parameter to its default value.
local-auth	Sets the Extensible Authentication Protocol (EAP) profile parameters and attributes to their default values.
mac-filtering	Sets the MAC filtering parameters and attributes to their default values.
media-stream	Sets the media stream parameters and attributes to their default values.

mfp	Sets the Management Frame Protection (MPF) parameters and attributes to their default values.
mobility	Sets the mobility parameters and attributes to their default values.
nac	Sets the RADIUS Network Admission Control (NAC) parameter to its default value.
passive-client	Sets the passive client parameter to its default value.
peer-blocking	Sets the peer to peer blocking parameters and attributes to their default values.
radio	Sets the radio policy parameters and attributes to their default values.
roamed-voice-client	Sets the roamed voice client parameters and attributes to their default values.
security	Sets the security policy parameters and attributes to their default values.
service-policy	Sets the WLAN quality of service (QoS) policy parameters and attributes to their default values.
session-timeout	Sets the client session timeout parameter to its default value.
shutdown	Sets the shutdown parameter to its default value.
sip-cac	Sets the Session Initiation Protocol (SIP) Call Admission Control (CAC) parameters and attributes to their default values.
static-ip	Sets the static IP client tunneling parameters and their attributes to their default values.
uapsd	Sets the Wi-Fi Multimedia (WMM) Unscheduled Automatic Power Save Delivery (UAPSD) parameters and attributes to their default values.
wgb	Sets the Workgroup Bridges (WGB) parameter to its default value.
wmm	Sets the WMM parameters and attributes to their default values.

Command Default

None.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

This example shows how to set the Cisco Client Extension parameter to its default value:

```
Device(config-wlan)# default ccx aironet-iesupport
```

daisychain-stp-redundancy

To enable redundant Root Access Point (RAP) ethernet daisy chaining on a mesh profile, use the **daisychain-stp-redundancy** command.

daisychain-stp-redundancy

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global Configuration

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.4.1	This command was introduced.

Usage Guidelines

This example shows how to enable redundant RAP ethernet daisy chaining on a mesh profile:

```
Device# configure terminal
Device(config)# wireless profile mesh default-mesh-profile
Device(config-wireless-mesh-profile)# daisychain-stp-redundancy
Device(config-wireless-mesh-profile)# end
```

debug platform qos-acl-tcam

To enable debugging of the quality of service (QoS) and access control list (ACL) hardware memory manager software, use the **debug platform qos-acl-tcam** command in privileged or user EXEC mode. To disable debugging, use the **no** form of this command.

debug platform qos-acl-tcam {**all** | **ctcam** | **errors** | **labels** | **mask** | **rpc** | **tcam**}
no debug platform qos-acl-tcam {**all** | **ctcam** | **errors** | **labels** | **mask** | **rpc** | **tcam**}

Syntax Description

all	Displays all QoS and ACL ternary content addressable memory (QATM) manager debug messages.
ctcam	Displays Cisco TCAM (CTCAM) related-events debug messages.
errors	Displays QATM error-related-events debug messages.
labels	Displays QATM label-related-events debug messages.
mask	Displays QATM mask-related-events debug messages.
rpc	Displays QATM remote procedure call (RPC) related-events debug messages.
tcam	Displays QATM hardware-memory-related events debug messages.

Command Default

Debugging is disabled.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

The **undebug platform qos-acl-tcam** command is the same as the **no debug platform qos-acl-tcam** command.

When you enable debugging on a switch stack, it is enabled only on the active switch. To enable debugging on a stack member, you can start a session from the active switch by using the **session** *switch-number* EXEC command. Then enter the **debug** command at the command-line prompt of the stack member. You also can use the **remote command** *stack-member-number LINE* EXEC command on the active switch to enable debugging on a member switch without first starting a session.

debug platform packet-trace

To enable conditional debugging packet tracing, use the **debug platform packet-trace** command in privileged or user EXEC mode. To disable debugging, use the **no** form of this command.

debug platform packet-trace {**copy** | **drop** | **inject** | **packet** | **punt** | **statistics**}
no debug platform packet-trace {**copy** | **drop** | **inject** | **packet** | **punt** | **statistics**}

Syntax Description

copy	Displays copy packet data.
drop	Displays trace drops only.
inject	Displays trace injects only.
packet	Displays packet count.
punt	Displays trace punts only.
statistics	Displays packet trace statistics.

Command Default

Debugging is disabled.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Usage Guidelines

The **undebug platform packet-trace** command is the same as the **no debug platform packet-trace** command.

For reference, see the following **Cisco ASR 1000 Series Aggregation Services Routers** documentation:

https://www.cisco.com/c/en/us/support/docs/content-networking/adaptive-session-redundancy-asr/117858-technote-asr-00.html

debug platform hardware chassis active qfp feature wireless datapath trace-buffer debug-level

To enables the debug level information for global and filtered logic, use the **debug platform hardware chassis active qfp feature wireless datapath trace-buffer debug-level** command. Use the **no** form of this command to disable the feature.

debug platform hardware chassis active qfp feature wireless datapath trace-buffer debug-level { **all** | **error** | **info** | **trace** | **warning** }

no debug platform hardware chassis active qfp feature wireless datapath trace-buffer debug-level { **all** | **error** | **info** | **trace** | **warning** }

Syntax Description

debug platform hardware chassis active qfp feature wireless datapath trace-buffer debug-level	Enables QFP wireless debug level.
all	Enables all debug.
error	Enables Error debug. Error is the default in the debug level.
info	Enables Info debug.
trace	Enables Trace debug.
warning	Enables Warning debug.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.6.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows you how to enable the debug level information for global and filtered logic:

```
Device# debug platform hardware chassis active qfp feature wireless datapath trace-buffer
debug-level all
```

debug platform hardware chassis active qfp feature wireless datapath trace-buffer ingress filtered-trace

To enables the Quantum Flow Processor on filtered trace buffer in the ingress path, use the **debug platform hardware chassis active qfp feature wireless datapath trace-buffer ingress filtered-trace** command. Use the **no** form of this command to disable the feature.

debug platform hardware chassis active qfp feature wireless datapath trace-buffer ingress { **filtered-trace** { **capwap** { *ipv4* | *ipv6* | **keepalive** } | **wlclient** { **ipv6-nd** | **ipv6-ra** | **mac-address** *H.H.H* } }

no debug platform hardware chassis active qfp feature wireless datapath trace-buffer ingress { **filtered-trace** { **capwap** { *ipv4* | *ipv6* | **keepalive** } | **wlclient** { **ipv6-nd** | **ipv6-ra** | **mac-address** *H.H.H* } }

Syntax Description

debug platform hardware chassis active qfp feature wireless datapath trace-buffer ingress filtered-trace	Enables QFP wireless ingress packet filtered trace.
capwap	Enables the condition for CAPWAP to log packet information to the filtered trace buffer.
wlclient	Enables the condition for wireless client to log packet information to the filtered trace buffer.
keepalive	Enables keepalive logging for all CAPWAP tunnels.
ipv4	Enables keepalive logging for the specified CAPWAP IPv4 address.
ipv6	Enables keepalive logging for the specified CAPWAP IPv6 address.
ipv6-nd	Enables IPv6 neighbor discovery for all wireless clients.
ipv6-ra	Enables IPv6 router advertisements for all wireless clients.
mac-address *H.H.H*	Enables packet logging for specified client MAC address.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.6.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows you how to enable the Quantum Flow Processor on filtered trace buffer in the ingress path:

```
Device# debug platform hardware chassis active qfp feature wireless datapath trace-buffer
ingress filtered-trace capwap ipv4 209.165.200.224/27
```

debug platform hardware chassis active qfp feature wireless datapath trace-buffer ingress global-trace

To enables the Quantum Flow Processor on global trace buffer in the ingress path, use the **debug platform hardware chassis active qfp feature wireless datapath trace-buffer ingress global-trace** command. Use the **no** form of this command to disable the feature.

debug platform hardware chassis active qfp feature wireless datapath trace-buffer ingress global-trace

no debug platform hardware chassis active qfp feature wireless datapath trace-buffer ingress global-trace

Syntax Description

debug platform hardware chassis active qfp feature wireless datapath trace-buffer ingress global-trace	Enables QFP wireless ingress packet global trace.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.6.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows you how to enable the Quantum Flow Processor on global trace buffer in the ingress path:

```
Device# debug platform hardware chassis active qfp feature wireless datapath trace-buffer
ingress global-trace
```

debug platform hardware chassis active qfp feature wireless datapath trace-buffer punt-inject filtered-trace

To enables the Quantum Flow Processor on filtered trace buffer in the ingress path, use the **debug platform hardware chassis active qfp feature wireless datapath trace-buffer punt-inject filtered-trace** command. Use the **no** form of this command to disable the feature.

debug platform hardware chassis active qfp feature wireless datapath trace-buffer punt-inject filtered-trace { **filtered-trace** { **capwap** { *ipv4* | *ipv6* | **keepalive** } | **wlclient** { **ipv6-nd** | **ipv6-ra** | **mac-address** *H.H.H* } }

no debug platform hardware chassis active qfp feature wireless datapath trace-buffer punt-inject filtered-trace { **filtered-trace** { **capwap** { *ipv4* | *ipv6* | **keepalive** } | **wlclient** { **ipv6-nd** | **ipv6-ra** | **mac-address** *H.H.H* } }

Syntax Description

debug platform hardware chassis active qfp feature wireless datapath trace-buffer punt-inject filtered-trace	Enables the filtered trace buffer in the punt-inject path.
capwap	Enables the condition for CAPWAP to log packet information to the filtered trace buffer in the punt-inject path.
wlclient	Enables the condition for wireless client to log packet information to the filtered trace buffer in the punt-inject path.
keepalive	Enables keepalive logging for all CAPWAP tunnels.
ipv4	Enables keepalive logging for the specified CAPWAP IPv4 address.
ipv6	Enables keepalive logging for the specified CAPWAP IPv6 address.
ipv6-nd	Enables IPv6 neighbor discovery for all wireless clients.
ipv6-ra	Enables IPv6 router advertisements for all wireless clients.
mac-address *H.H.H*	Enables packet logging for specified client MAC address.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.6.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows you how to enable the Quantum Flow Processor on filtered trace buffer in the punt-inject path:

```
Device# debug platform hardware chassis active qfp feature wireless datapath trace-buffer
punt-inject filtered-trace capwap ipv4 209.165.200.224/27
```

debug platform hardware chassis active qfp feature wireless datapath trace-buffer punt-inject global-trace

To enable the Quantum Flow Processor on global trace buffer in the punt-inject path, use the **debug platform hardware chassis active qfp feature wireless datapath trace-buffer punt-inject global-trace** command. Use the **no** form of this command to disable the feature.

debug platform hardware chassis active qfp feature wireless datapath trace-buffer punt-inject global-trace

no debug platform hardware chassis active qfp feature wireless datapath trace-buffer punt-inject global-trace

Syntax Description

debug platform hardware chassis active qfp feature wireless datapath trace-buffer punt-inject global-trace	Enables the Quantum Flow Processor on global trace buffer in the punt-inject path.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.6.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows you how to enables the Quantum Flow Processor on global trace buffer in the punt-inject path:

```
Device# debug platform hardware chassis active qfp feature wireless datapath trace-buffer
punt-inject global-trace
```

debug qos-manager

To enable debugging of the quality of service (QoS) manager software, use the **debug qos-manager** command in privileged EXEC mode. Use the **no** form of this command to disable debugging.

debug qos-manager {**all** | **event** | **verbose**}
no debug qos-manager {**all** | **event** | **verbose**}

Syntax Description

all	Display all QoS-manager debug messages.
event	Display QoS-manager related-event debug messages.
verbose	Display QoS-manager detailed debug messages.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

The **undebug qos-manager** command is the same as the **no debug qos-manager** command.

debug wireless bundle client abort

To cancel the collection of debug bundles for wireless clients, use the **debug wireless bundle client abort** command.

debug wireless bundle client abort

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Dublin 17.9.3	This command was introduced.

Usage Guidelines

You can run the **abort** command only after 60 seconds of running the **start** command. The **abort** command cannot be used after the **stop** command is issued.

Examples

The following example shows how to cancel the collection of debug bundles for wireless clients:

```
Device# debug wireless bundle client abort
```

debug wireless bundle client mac

To add the client MAC addresses from which the wireless client debug logs are required, use the **debug wireless bundle client mac** command. Use the **no** form of this command to remove the MAC addresses.

debug wireless bundle client mac *mac-address*

no debug wireless bundle client mac *mac-address*

Syntax Description

mac-address	Specifies the MAC address of the client.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Dublin 17.9.3	This command was introduced.

Usage Guidelines

You can specify up to 32 client MAC addresses.

For example, **debug wireless bundle client mac***F8XX.F2XX.7DXXaaaa.bbbb.cccc*

Examples

This example shows how to add the client MAC addresses from which the wireless client debug logs should be collected:

```
Device# debug wireless bundle client mac F8XX.F2XX.7DXX
```

debug wireless bundle client start

To start collecting the debug bundle for wireless clients, use the **debug wireless bundle client start** command.

debug wireless bundle client start { **ap-archive** [**site-tag** *site_tag* **level** { **critical** | **debug** | **error** | **verbose** }] | **epc** | **monitor-time** *monitor-time-seconds* }

debug wireless bundle client start { **epc** | **monitor-time** *monitor-time-seconds* }

Syntax Description

ap-archive	Enables the AP archive in a site tag.
site-tag *site_tag*	Specifies the site tag name to enable AP archive.
level	Specifies the AP archive level.
critical	Specifies the critical level of AP archive.
debug	Specifes the debug level of AP archive.
error	Specifies the error level of AP archive.
verbose	Specifies the verbose level of AP archive.
epc	Enables the embedded packet capture in the control plane.
monitor-time	Specifies the duration to trace the monitor time. The default time range is 30 minutes. The valid values range from 1 to 2085978494.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Dublin 17.9.3	This command was introduced.

Examples

The following example shows how to start the collection of the debug bundle for wireless clients:

```
Device# debug wireless bundle client start epc monitor-time 30
Device# debug wireless bundle client start ap-archive site-tag default-site-tag level debug
```

debug wireless bundle client stop-all collect

To stop the collection of the debug bundles for all configured wireless clients, use the **debug wireless bundle client stop-all collect** command.

debug wireless bundle client stop-all collect { **all** | **mac** *H.H.H* }

Syntax Description

all	Collects the debug bundles for all the configured wireless clients.
mac	Collects the debug bundles for client devices whose MAC addresses are added. You can enter a maximum of five MAC addresses.
HHH	Specifies the client MAC addresses.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Dublin 17.9.3	This command was introduced.

Examples

The example shows how to stop the collection of the debug bundles for all configured wireless clients:

```
Device# debug wireless bundle client stop-all collect all
```

description

To configure a description for a flow monitor, flow exporter, or flow record, use the **description** command in the appropriate configuration mode. To remove a description, use the **no** form of this command.

description *description*
no description *description*

Syntax Description

description	Text string that describes the flow monitor, flow exporter, or flow record.

Command Default

The default description for a flow sampler, flow monitor, flow exporter, or flow record is "User defined."

Command Modes

The following command modes are supported:

Flow exporter configuration

Flow monitor configuration

Flow record configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

To return this command to its default setting, use the **no description** or **default description** command in the appropriate configuration mode.

The following example configures a description for a flow monitor:

```
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)# description Monitors traffic to 172.16.0.1 255.255.0.0
```

destination

To configure an export destination for a flow exporter, use the **destination** command in flow exporter configuration mode. To remove an export destination for a flow exporter, use the **no** form of this command.

destination {*hostnameip-address*}
no destination {*hostnameip-address*}

Syntax Description

hostname	Hostname of the device to which you want to send the NetFlow information.
ip-address	IPv4 address of the workstation to which you want to send the NetFlow information.

Command Default

An export destination is not configured.

Command Modes

Flow exporter configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

Each flow exporter can have only one destination address or hostname.

When you configure a hostname instead of the IP address for the device, the hostname is resolved immediately and the IPv4 address is stored in the running configuration. If the hostname-to-IP-address mapping that was used for the original Domain Name System (DNS) name resolution changes dynamically on the DNS server, the device does not detect this, and the exported data continues to be sent to the original IP address, resulting in a loss of data.

To return this command to its default setting, use the **no destination** or **default destination** command in flow exporter configuration mode.

The following example shows how to configure the networking device to export the cache entry to a destination system:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# destination 10.0.0.4
```

device-role (IPv6 snooping)

To specify the role of the device attached to the port, use the **device-role** command in IPv6 snooping configuration mode.

device-role {**node** | **switch**}

Syntax Description

node	Sets the role of the attached device to node.
switch	Sets the role of the attached device to switch.

Command Default

The device role is node.

Command Modes

IPv6 snooping configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

The **device-role** command specifies the role of the device attached to the port. By default, the device role is node.

The **switch** keyword indicates that the remote device is a switch and that the local switch is now operating in multiswitch mode; binding entries learned from the port will be marked with trunk_port preference level. If the port is configured as a trust-port, binding entries will be marked with trunk_trusted_port preference level.

This example shows how to define an IPv6 snooping policy name as policy1, place the device in IPv6 snooping configuration mode, and configure the device as the node:

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# device-role node
```

device-role (IPv6 nd inspection)

To specify the role of the device attached to the port, use the **device-role** command in neighbor discovery (ND) inspection policy configuration mode.

device-role {**host** | **monitor** | **router** | **switch**}

Syntax Description

host	Sets the role of the attached device to host.
monitor	Sets the role of the attached device to monitor.
router	Sets the role of the attached device to router.
switch	Sets the role of the attached device to switch.

Command Default

The device role is host.

Command Modes

ND inspection policy configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
	The keywords **monitor** and **router** are deprecated.

Usage Guidelines

The **device-role** command specifies the role of the device attached to the port. By default, the device role is host, and therefore all the inbound router advertisement and redirect messages are blocked. If the device role is enabled using the **router** keyword, all messages (router solicitation [RS], router advertisement [RA], or redirect) are allowed on this port.

When the **router** or **monitor** keyword is used, the multicast RS messages are bridged on the port, regardless of whether limited broadcast is enabled. However, the monitor keyword does not allow inbound RA or redirect messages. When the monitor keyword is used, devices that need these messages will receive them.

The **switch** keyword indicates that the remote device is a switch and that the local switch is now operating in multiswitch mode; binding entries learned from the port will be marked with trunk_port preference level. If the port is configured as a trust-port, binding entries will be marked with trunk_trusted_port preference level.

The following example defines a Neighbor Discovery Protocol (NDP) policy name as policy1, places the device in ND inspection policy configuration mode, and configures the device as the host:

```
Device(config)#  ipv6 nd inspection policy policy1
Device(config-nd-inspection)# device-role host
```

device-tracking binding

To configure the timer values for the IP entries of wireless clients in different states, use the **device-tracking binding** command. To disable the configured timer values for the IP entries, use the **no** form of this command.

device-tracking binding { **down-lifetime** | **reachable-lifetime** | **stale-lifetime** } { *seconds* | **infinite** }

no device-tracking binding { **down-lifetime** | **reachable-lifetime** | **stale-lifetime** }

Syntax Description

down-lifetime	Specifies the maximum time in down state before removal of the IP binding entry.
reachable-lifetime	Specifies the maximum time in reachable state without any activity for an IP binding entry.
stale-lifetime	Specifies the maximum time in stale state before deletion of an IP binding entry.
seconds	The timer value for the IP entries, in seconds. The valid range is from 1 to 86400 seconds.
infinite	Indicates that the timer interval does not expire.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.3.1.	This command was introduced in a release earlier than Cisco IOS XE Amsterdam 17.3.1.

Examples

The following example shows how to configure the timer values for the IP entries of wireless clients in different states:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# device-tracking binding stale-lifetime 3
```

device-tracking binding vlan

To configure IPv4 or IPv6 static entry, use the **device-tracking binding vlan** command.

device-tracking binding vlan *vlan-id* {*ipv4-addr ipv6-addr* }**interface gigabitEthernet** *ge-intf-num hardware-or-mac-address*

Syntax Description

vlan-id	VLAN ID. Valid range is 1 to 4096.
ipv4-addr	IPv4 address of the device.
ipv6-addr	IPv6 address of the device.
interface gigabitEthernet	GigabitEthernet IEEE 802.3z.
ge-intf-num	GigabitEthernet interface number. Valid range is 1 to 32.
hardware-or-mac-address	The 48-bit hardware address or the MAC address of the device.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure IPv4 static entry:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# device-tracking binding vlan 20 20.20.20.5 interface gigabitEthernet 1
0000.1111.2222
```

device-tracking policy

To configure a Switch Integrated Security Features (SISF)-based IP device tracking policy, use the **device-tracking** command in global configuration mode. To delete a device tracking policy, use the **no** form of this command.

device -tracking policy *policy-name*
no device-tracking policy *policy-name*

Syntax Description

policy-name	User-defined name of the device tracking policy. The policy name can be a symbolic string (such as Engineering) or an integer (such as 0).

Command Default

A device tracking policy is not configured.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

Use the SISF-based **device-tracking policy** command to create a device tracking policy. When the **device-tracking policy** command is enabled, the configuration mode changes to device-tracking configuration mode. In this mode, the administrator can configure the following first-hop security commands:

- (Optional) **device-role**{**node**] | **switch**}—Specifies the role of the device attached to the port. Default is **node**.
- (Optional) **limit address-count** *value*—Limits the number of addresses allowed per target.
- (Optional) **no**—Negates a command or sets it to defaults.
- (Optional) **destination-glean**{**recovery**| **log-only**}[**dhcp**]}—Enables binding table recovery by data traffic source address gleaning.
- (Optional) **data-glean**{**recovery**| **log-only**}[**dhcp** | **ndp**]}—Enables binding table recovery using source or data address gleaning.
- (Optional) **security-level**{**glean**|**guard**|**inspect**}—Specifies the level of security enforced by the feature. Default is **guard.**

  glean—Gleans addresses from messages and populates the binding table without any verification.
  guard—Gleans addresses and inspects messages. In addition, it rejects RA and DHCP server messages. This is the default option.
  inspect—Gleans addresses, validates messages for consistency and conformance, and enforces address ownership.
- (Optional) **tracking** {**disable** | **enable**}—Specifies a tracking option.
- (Optional) **trusted-port**—Sets up a trusted port. It disables the guard on applicable targets. Bindings learned through a trusted port have preference over bindings learned through any other port. A trusted port is given preference in case of a collision while making an entry in the table.

This example shows how to configure an a device-tracking policy:

```
Device(config)# device-tracking policy policy1
Device(config-device-tracking)# trusted-port
```

description word

To configure and specify the description of the RF profile, use the **description word** command in the global configuration mode. Use the **no** form of this command to disable the feature.

description word

no description word

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Cisco IOS XE 26.1.1	This command is introduced.

Examples

This example shows how to configure and specify the description of the RF profile in the global configuration mode:

```
Device# configure terminal
Device(config)# ap dot11
Device(config)# ap dot11 24ghz
Device(config)# ap dot11 24ghz rf-profile
Device(config)# ap dot11 24ghz rf-profile default-rf-profile
Device(config)# description description-word
Device(config)# exit
```

destination-ports

To configure a destination port to communicate with the controller, use the **destination-ports** command. To disable the port used to communicate with the controller, use the **no** form of this command.

destination-ports { **application-updates** | **sensor-exporter** } *port-value*

no destination-ports { **application-updates** | **sensor-exporter** }

Syntax Description

application-updates	Configures the TCP port for application updates.
sensor-exporter	Configures the UDP port for sensor messages.
port-value	Port value. Valid range is from 1 to 65535.

Command Default

Destination port is not configured.

Command Modes

SD Service Controller Configuration (config-sd-service-controller)

Command History

Release	Modification
Cisco IOS XE Cupertino 17.7.1	This command was introduced.

Examples

The following example shows how to configure a destination port for communicating with the controller:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
VM1(config)# avc sd-service
Device(config-sd-service)# controller
Device(config-sd-service-controller)# destination-ports application-updates 650
```

dhcp broadcast

To enable DHCP broadcast for locally switched profiles, use the **dhcp broadcast** command.

dhcp broadcast

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Wireless FlexConnect profile configuration mode

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.4.x	This command was introduced.

Examples

The following example shows how to enable dhcp broadcast for locally switched clients:

```
Device# configure terminal
Device(config)# wireless profile flex default-flex-profile
Device(config-wireless-flex-profile)# dhcp broadcast
```

dhcp-server

To enable DHCP server for a Cisco AP profile, use the **dhcp-server** command.

dhcp-server

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global Configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Usage Guidelines

This example shows how to enable DHCP server for a Cisco AP profile:

```
Device# configure terminal
Device(config)# ap profile ap-prof1
Device(config-ap-profile)# dhcp-server
```

dhcp-tlv-caching

To configure DHCP TLV caching on a WLAN, use the **dhcp-tlv-caching** command.

dhcp-tlv-caching

Command Default None

Command Modes config-wireless-policy

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Example

This example shows how to configure DHCP TLV caching on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy rr-xyz-policy-1
Device(config-wireless-policy)# dhcp-tlv-caching
Device(config-wireless-policy)# radius-profiling
Device(config-wireless-policy)# end
```

dns-server (IPv6)

To specify the Domain Name System (DNS) IPv6 servers available to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **dns-server** command in DHCP for IPv6 pool configuration mode. To remove the DNS server list, use the **no** form of this command.

dns-server *ipv6-address*
no dns-server *ipv6-address*

Syntax Description

ipv6-address	The IPv6 address of a DNS server. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

Command Default

When a DHCP for IPv6 pool is first created, no DNS IPv6 servers are configured.

Command Modes

DHCP for IPv6 pool configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

Multiple Domain Name System (DNS) server addresses can be configured by issuing this command multiple times. New addresses will not overwrite old addresses.

Examples

The following example specifies the DNS IPv6 servers available:

```
dns-server 2001:0DB8:3000:3000::42
```

Related Commands

Command	Description
domain-name	Configures a domain name for a DHCP for IPv6 client.
ipv6 dhcp pool	Configures a DHCP for IPv6 configuration information pool and enters DHCP for IPv6 pool configuration mode.

dnscrypt

To enable or disable DNScrypt, use the **dnscrypt** command.

dnscrypt

Command Default None

Command Modes config-profile

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines By default, the DNScrypt option is enabled.

This example shows how to enable or disable DNScrypt:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# parameter-map type umbrella global
Device(config-profile)# token 57CC80106C087FB1B2A7BAB4F2F4373C00247166
Device(config-profile)# local-domain dns_wl
Device(config-profile)# no dnscrypt
Device(config-profile)# end
```

domain

To configure a 802.11u domain name, use the **domain** command. To remove domain name, use the **no** form of the command.

domain *domain-name*

Syntax Description

domain-name	802.11u domain name. You can configure up to 32 domain names. The *domain-name* should not exceed 220 characters.

Command Default

None

Command Modes

Wireless ANQP Server Configuration (config-wireless-anqp-server)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Example

The following example shows how to configure a 802.11u domain name:

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# domain my-domain
```

domain-name (DHCP)

To specify the domain n ame for a Dynamic Host Configuration Protocol (DHCP) client, use the **domain-name** command in DHCP pool configuration mode. To remove the domain name, use the no form of this command.

domain-name *domain*
no domain-name

Syntax Description

domain	Specifies the domain name string of the client.

Command Default

No default behavior or values.

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example specifies cisco.com as the domain name of the client:

```
domain-name cisco.com
```

Related Commands

Command	Description
dns-server	Specifies the DNS IP servers available to a DHCP client.
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.

dot11 24ghz | 5ghz data rate min

To configure the minimum data rate for 2.4 GHz and 5 GHz radio on your WLAN, use the **dot11** { **24ghz** | **5ghz** } **data rate min** command in the WLAN configuration mode. Use the **no** form of this command to disable the feature.

ap dot11 { **24ghz** | **5ghz** } **data rate min**

no ap dot11 { **24ghz** | **5ghz** } **data rate min**

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

WLAN configuration mode

Command History

Release	Modification
Cisco IOS XE 26.1.1	This command is introduced.

Usage Guidelines

If the SSID minimum data rate does not have a higher mandatory rate, the system will advertise the next available mandatory rate from the RF profile that is lower than the minimum data rate.

Examples

This example shows how to configure the minimum data rate for 2.4 GHz radio on your WLAN in the WLAN configuration mode:

```
Device# configure terminal
Device(config)# wlan default-wlan-profile
Device(config)# wlan default-wlan-profile 4000 SSID50
Device(config-wlan)# dot11 24ghz data-rate
Device(config-wlan)# dot11 24ghz data-rate min RATE_9M
Device(config-wlan)# exit
```

This example shows how to configure the minimum data rate for 5 GHz radio on your WLAN in the WLAN configuration mode:

```
Device# configure terminal
Device(config)# wlan default-wlan-profile
Device(config)# wlan default-wlan-profile 4000 SSID50
Device(config-wlan)# dot11 5ghz data-rate
Device(config-wlan)# dot11 5ghz data-rate min RATE_12M
Device(config-wlan)# exit
```

dot11 {24ghz | 5ghz | 6ghz} slot0 radio-profile

To configure 802.11a and 802.11b radio profile for slot 0, use the **dot11 {24ghz | 5ghz | 6ghz} slot0 radio-profile** command.

dot11 { **24ghz** | **5ghz** | **6ghz** } **slot0 radio-profile**

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Wireless RF tag configuration (config-wireless-rf-tag)

Command History

Release	Modification
Cisco IOS XE Cupertino 17.18.2	This command is introduced.

Examples

This example shows how to configure 802.11a and 802.11b radio profile for slot 0 in the wireless RF tag configuration mode:

```
Device# configure terminal
Device(config)# wireless tag rf default-rf-tag
Device(config-wireless-rf-tag)# dot11 {24ghz | 5ghz | 6hz} slot0 radio-profile RF-profile
Device(config-wireless-rf-tag)# end
```

dot11 5ghz slot1 radio-profile

To configure 802.11a radio profile for slot 1, use the **dot11 5ghz slot1 radio-profile** *radio-profile-name*

dot11 5ghz slot1 radio-profile *radio-profile-name*

Syntax Description

radio-profile-name	Specifies the name of the radio profile.

Command Default

None

Command Modes

Wireless RF tag configuration (config-wireless-rf-tag)

Command History

Release	Modification
Cisco IOS XE 17.18.1	This command was introduced.

Examples

The following example shows how to configure 802.11a radio profile for slot 1:

```
Device# configure terminal
Device(config)# wireless tag rf rf-tag-name
Device(config-wireless-rf-tag)# dot11 5GHz slot1 radio-profile radio-name
```

dot11 airtime-fairness

To configure airtime-fairness policy for 2.4- or 5-GHz radio, use the **dot11 airtime-fairness** command.

dot11 { **24ghz** | **5ghz** } **airtime-fairness** *atf-policy-name*

Syntax Description

atf-policy-name	Is the name of the airtime-fairness policy.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

This example shows how to configure airtime-fairness policy for 2.4- or 5-GHz radio:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy <profile-name>
Device(config-wireless-policy)# dot11 24ghz airtime-fairness <atf-policy-name>
Device(config-wireless-policy)# end
```

dot11be-profile

To configure the 802.11be profile in a WLAN, use the **dot11be-profile** command.

dot11be-profile *default-dot11be-profile*

Syntax Description

default-dot11be-profile	Specifies the name of the 802.11be profile in a WLAN.

Command Default

None

Command Modes

WLAN configuration mode

Command History

Release	Modification
Cisco IOS XE 17.15.1	This command was introduced.

Examples

The following example shows you how to configure a 802.11be profile in a WLAN:

```
Device# configure terminal
Device(config# wlan wlan-dot11be-profile
Device(config-wlan)# dot11be-profile default-dot11be-profile
```

dot11 a-mpdu tx block-ack window-size

To configure the 802.11 transmit Aggregated MAC Protocol Data Unit (A-MPDU) window size, use the **dot11 a-mpdu tx block-ack window-size** command.

dot11 a-mpdu tx block-ack window-size *1-255*

Syntax Description

1-255	Sets the maximum number of MAC PDUs aggregated in a single A-MPDU.

Command Default

None

Command Modes

RF configuration mode

Command History

Release	Modification
Cisco IOS XE 17.15.1	This command was introduced.

Examples

This example shows how to configure the 802.11 transmit A-MPDU window size:

```
Device# configure terminal
Device(config)# ap dot11 6ghz rf-profile rf-ampdu-profile
Device(config-rf-profile)# dot11 a-mpdu tx block-ack window-size 255
```

dot11ax

To configure 802.11ax on a WLAN, use the **dot11ax** command.

dot11ax { **bss-colorcode** *color-code-range* | **bss-colormode** | **bss-partialcolor** | **downlink-mumimo** | **downlink-ofdma** | **target-waketime** | **twt-broadcast-support** | **uplink-mumimo** | **uplink-ofdma** }

Syntax Description

bss-colorcode	BSS color code on a WLAN.
color-code-range	BSS color code range. Valid range is from 0-255.
bss-colormode	BSS color mode on a WLAN.
bss-partialcolor	BSS patrial color mode on a WLAN.
downlink-mumimo	Downlink MUMIMO on a WLAN.
downlink-ofdma	Downlink OFDMA on a WLAN.
target-waketime	Target wake time mode on a WLAN.
twt-broadcast-support	TWT broadcast support on a WLAN.
uplink-mumimo	Uplink MUMIMO on a WLAN.
uplink-ofdma	Uplink OFDMA on a WLAN.

Command Default

None

Command Modes

WLAN Configuration (config-wlan)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

This command is supported only on IEEE 802.11ax APs.

Example

The following example shows how to configure uplink OFDMA on a WLAN.

```
Device(config-wlan)# dot11ax uplink-ofdma
```

dot11ax bcast-probe-response

To configure the 802.11ax broadcast probe response, use the **dot11ax bcast-probe-response** command. Use the **no** form of this command to disable this feature.

dot11ax bcast-probe-response

no dot11ax bcast-probe-response

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

RF configuration mode

Command History

Release	Modification
Cisco IOS XE Cupertino 17.7.1	This command was introduced.

Example

The following example shows how to configure 802.11ax broadcast probe response:

```
Device(config)# ap dot11 6ghz rf-profile rf-profile-name
Device(config-rf-profile)# dot11ax bcast-probe-response
```

dot11ax bcast-probe-response time-interval

To configure the 802.11ax broadcast probe response interval, use the **dot11ax bcast-probe-response time-interval** command. Use the **no** form of this command to disable this feature.

dot11ax bcast-probe-response time-interval *5-25*

no dot11ax bcast-probe-response time-interval *5-25*

Syntax Description

5-25	Specifies the broadcast probe response time interval.

Command Default

None

Command Modes

RF configuration mode

Command History

Release	Modification
Cisco IOS XE Cupertino 17.7.1	This command was introduced.

Example

The following example shows how to configure 802.11ax broadcast probe response interval:

```
Device(config)# ap dot11 6ghz rf-profile rf-profile-name
Device(config-rf-profile)# dot11ax bcast-probe-response time-interval 25
```

dot11ax fils-discovery

To configure the 802.11ax fast initial link setup (FILS) discovery frame for broadcast, use the **dot11ax fils-discovery** command. Use the **no** form of this command to disable this feature.

dot11ax fils-discovery

no dot11ax fils-discovery

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

RF configuration mode

Command History

Release	Modification
Cisco IOS XE Cupertino 17.7.1	This command was introduced.

Example

The following example shows how to configure 802.11ax fast initial link setup (FILS) discovery frame for broadcast :

```
Device(config)# ap dot11 6ghz rf-profile rf-profile-name
Device(config-rf-profile)# dot11ax fils-discovery
```

dot11ax multi-bssid-profile

To configure the 802.11ax multi BSSID profile name, use the **dot11ax multi-bssid-profile**. Use the **no** form of this command to disable this feature.

dot11ax multi-bssid-profile *multi-bssid-profilename*

no dot11ax multi-bssid-profile *multi-bssid-profilename*

Syntax Description

multi-bssid-profilename	Specifies the multi BSSID profile name.

Command Default

None

Command Modes

RF configuration mode

Command History

Release	Modification
Cisco IOS XE Cupertino 17.7.1	This command was introduced.

Example

The following example shows how to configure the 802.11ax multi BSSID profile name:

```
Device(config)# ap dot11 6ghz rf-profile rf-profile-name
Device(config-rf-profile)# dot11ax multi-bssid-profile multi-bssid-profilename
```

dot11ax spatial-reuse obss-pd

To configure 802.11ax OBSS PD max in the RF profile configuration mode, use the **dot11ax spatial-reuse obss-pd**

dot11ax spatial-reuse obss-pd

no dot11ax spatial-reuse obss-pd

Syntax Description

spatial-reuse obss-pd	Configures 802.11ax OBSS PD based spatial reuse in the RF profile configuration mode.

Command Default

None

Command Modes

RF profile configuration

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.4.1	This command was introduced.

Example

The following example shows how to configures 802.11ax OBSS PD based spatial reuse in the RF profile configuration mode:

```
Device(config-rf-profile)# dot11ax spatial-reuse obss-pd
```

dot11ax spatial-reuse obss-pd non-srg-max

To configure 802.11ax non-SRG OBSS PD max in the RF profile configuration mode, use the **dot11ax spatial-reuse obss-pd non-srg-max** *-82 - -62*

dot11ax spatial-reuse obss-pd non-srg-max *-82 - -62*

no dot11ax spatial-reuse obss-pd non-srg-max *-82 - -62*

Syntax Description

spatial-reuse obss-pd non-srg-max	Configures 802.11ax non-SRG OBSS PD based spatial reuse in the RF profile configuration mode.
-82 - -62	Sprcifies the non-SRG OBSS PD max value in dBm

Command Default

None

Command Modes

RF profile configuration

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.4.1	This command was introduced.

Example

The following example shows how to configures 802.11ax non-SRG OBSS PD based spatial reuse in the RF profile configuration mode:

```
Device(config-rf-profile)# dot11ax spatial-reuse obss-pd non-srg-max -80
```

dot11ax target-waketime

To configure target wake time mode on WLAN, use the **dot11ax target-waketime** command. To disable the feature, use the **no** command of the command.

dot11ax target-waketime

[no] dot11ax target-waketime

Syntax Description

target-waketime	Configures target wake time mode on WLAN.

Command Default

None

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.2.1	This command was introduced.

Example

This example shows how to configure target wakeup time on WLAN:

```
Device(config-wlan)# dot11ax target-waketime
```

dot11ax twt-broadcast-support

To configure TWT broadcast support on WLAN, use the **dot11ax twt-broadcast-support** command. To disable the feature, use the **no** command of the command.

dot11ax twt-broadcast-support

[no] dot11ax twt-broadcast-support

Syntax Description

dot11ax twt-broadcast-support	Configures the TWT broadcast support on WLAN

Command Default

None

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.2.1	This command was introduced.

Example

This example shows how to configure target wakeup time on WLAN:

```
Device(config-wlan)# dot11ax twt-broadcast-support
```

dot11 {24ghz slot0 | 5ghz {slot1 | slot2} radio-profile

Configures 802.11a or 802.11b radio profile, use the **dot11** {**24ghz slot0** | **5ghz** {**slot1** | **slot2**}}**radio-profile** *radio-profile-name* command. Use the **no** form of this command to disable the feature.

dot11 { **24ghz slot0** | **5ghz** { **slot1** | **slot2** } } **radio-profile** *radio-profile-name*

no dot11 { **24ghz slot0** | **5ghz** { **slot1** | **slot2** } } **radio-profile** *radio-profile-name*

Syntax Description

dot11{**24ghz slot0** | **5ghz** {**slot1** | **slot2**}}	• **dot11**: Configures 802.11 parameters. • **24ghz slot0**: Configures 802.11b policy for slot 0. • **5ghz**: Configures 802.11a parameters. • **slot1**: Configures 802.11a policy for slot 1. • **slot2**: Configures 802.11a policy for slot 2.
radio-profile	Configures the 802.11a or 802.11a radio profiles.
radio-profile-name	Specifies the 802.11a or 802.11a radio profile names.

Command Default

None

Command Modes

Wireless RF tag configuration mode

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.6.1	This command was introduced.

Usage Guidelines

None

Example

The following example shows you how to configure the 802.11a or 802.11b radio profile:

```
Device# configure terminal
Device(config)# wireless tag rf wireless-rf-tagname
Device(config-wireless-rf-tag)# dot11 5ghz slot1 radio-profile wireless-radio-profile
```

dot11bg 11g

To connect only 802.11g clients to the WLAN on the 2.4-GHz band, use the **dot11bg 11g** command.

dot11bg 11g

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.6.1	This command was introduced.

Usage Guidelines

The **dot11bg 11g** is a newly introduced command compared to **radio dot11bg** and **radio dot11g** commands. The configuration applied through the new **dot11bg 11g** command takes precedence over the other older commands. This is applicable specifically to the 2.4-GHz band and does not impact other bands.

Examples

The following example shows how to connect only 802.11g clients to the WLAN on the 2.4-GHz band:

```
Device # configure terminal
Device (config)# wlan wlan-test 4 ssid-name
Device (config-wlan)# broadcast-ssid
Device (config-wlan)# dot11bg 11g
```

dot11 5ghz reporting-interval

To configure the client report interval sent from AP for clients on 802.11a radio, use the **dot11 5ghz reporting-interval** command.

dot11 5ghz reporting-interval *reporting-interval*

Syntax Description

reporting-interval	Interval at which client report needs to be sent in seconds.

Command Default

None

Command Modes

config-ap-profile

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to set the client report interval in seconds:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap profile profile-name
Device(config-ap-profile)# dot11 5ghz reporting-interval 8
```

dot11 reporting-interval

To set the volume metering interval, use the **dot11 reporting-interval** command.

dot11 { **24ghz** | **5ghz** } *reporting-interval*

Syntax Description

reporting-interval	Interval to send client accounting statistics.

Command Default

Interval is configured at the default level of 90 seconds.

Command Modes

config-ap-profile

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

Though the CLI allows you to configure range from 5 to 90 seconds, we recommend that you use 60 to 90 seconds range for Volume Metering.

This CLI can also be used to configure the interval when smart roam is enabled, which has a range of 5 to 90 seconds.

Though you can set two different values for volume metering and smart roam, only one value takes effect based on the order of execution. So, we recommend that you use the same reporting interval for both.

Example

The following example shows how to configure volume metering:

```
Device(config-ap-profile)# dot11 24ghz 60
```

dot1x system-auth-control

To globally enable 802.1X SystemAuthControl (port-based authentication), use the **dot1x system-auth-control**command in global configuration mode. To disable SystemAuthControl, use the **no** form of this command.

dot1x system-auth-control
no dot1x system-auth-control

Syntax Description

This command has no arguments or keywords.

Command Default

System authentication is disabled by default. If this command is disabled, all ports behave as if they are force authorized.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(2)XA	This command was introduced.
12.2(14)SX	This command was implemented on the Supervisor Engine 720.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The IEEE 802.1x standard defines a client-server-based access control and authentication protocol that restricts unauthorized devices from connecting to a LAN through publicly accessible ports. 802.1x controls network access by creating two distinct virtual access points at each port. One access point is an uncontrolled port; the other is a controlled port. All traffic through the single port is available to both access points. 802.1x authenticates each user device that is connected to a switch port and assigns the port to a VLAN before making available any services that are offered by the switch or the LAN. Until the device is authenticated, 802.1x access control allows only Extensible Authentication Protocol (EAP) over LAN (EAPOL) traffic through the port to which the device is connected. After authentication is successful, normal traffic can pass through the port.

The **no** form of the command removes any 802.1X-related configurations.

You must enable Authentication, Authorization, and Accounting (AAA) and specify the authentication method list before enabling 802.1X. A method list describes the sequence and authentication methods to be queried to authenticate a user.

Examples

The following example shows how to enable SystemAuthControl:

```
Router(config)# dot1x system-auth-control
```

Related Commands

Command	Description
aaa authentication dot1x	Specifies one or more AAA methods for use on interfaces running IEEE 802.1X.
aaa new-model	Enables the AAA access-control model.
debug dot1x	Displays 802.1X debugging information.
description	Specifies a description for an 802.1X profile.
device	Statically authorizes or rejects individual devices.
dot1x initialize	Initializes 802.1X state machines on all 802.1X-enabled interfaces.
dot1x max-req	Sets the maximum number of times that a router or Ethernet switch network module can send an EAP request/identity frame to a client (assuming that a response is not received) before restarting the authentication process.
dot1x port-control	Enables manual control of the authorized state of a controlled port.
dot1x re-authenticate	Manually initiates a reauthentication of the specified 802.1X-enabled ports.
dot1x reauthentication	Globally enables periodic reauthentication of the client PCs on the 802.1X interface.
dot1x timeout	Sets retry timeouts.
identity profile	Creates an identity profile and enters identity profile configuration mode.
show dot1x	Displays details and statistics for an identity profile.
template	Specifies a virtual template from which commands may be cloned.

dot11-tlv-accounting

To configure client 802.11 type, length, value (TLV) accounting, use the **dot11-tlv-accounting** command. To disable client 802.11 TLV accounting, use the **no** form of this command.

dot11-tlv-accounting

Syntax Description

This command has no keywords or arguments.

Command Default

Client 802.11 TLV accounting is not configured.

Command Modes

Wireless policy configuration (config-wireless-policy)#

Command History

Release	Modification
Cisco IOS XE Dublin 17.10.1	This command was introduced.

Examples

The following example shows how to configure client 802.11 TLV accounting:

```
Device# configure terminal
Device(config)# wireless profile policy default-policy-profile
Device(config-wireless-policy)# dot11-tlv-accounting
```

dscp

To enable differentiated services code point (DSCP) marking, use the **dscp** command. To disable DSCP marking, use the **no** form of this command.

dscp *dscp-value*

no dscp

Syntax Description

dscp-value	DSCP marking value. Valid range is from 0 to 63.

Command Default

DSCP marking is not enabled.

Command Modes

SD Service Controller Configuration (config-sd-service-controller)

Command History

Release	Modification
Cisco IOS XE Cupertino 17.7.1	This command was introduced.

Examples

The following example shows how to enable DSCP marking:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# avc sd-service
Device(config-sd-service)# controller
Device(config-sd-service-controller)# dscp 12
```

dual-mode-ap-deployment-mode

To configure the deployment mode of AP as either Indoor or Outdoor, use the **dual-mode-ap-deployment-mode** command. To revert the behavior of this command, use the **no** form of this command.

dual-mode-ap-deployment-mode { indoor | outdoor }

no dual-mode-ap-deployment-mode { indoor | outdoor }

Syntax Description

indoor	The AP joins the controller and works in the Indoor mode.
outdoor	The AP joins the controller and works in the Outdoor mode.

Command Default

Outdoor

Command Modes

AP profile configuration (config-ap-profile)

Command History

Release	Modification
Cisco IOS XE 17.13.1	This command was introduced.

Usage Guidelines

The AP joins the controller with its default mode.

This command is applicable only to Cisco Catalyst 9124AX Series Outdoor APs.

Examples

This example shows how to configure the deployment mode of an AP as Indoor:

```
Device# configure terminal
Device(config)# ap profile ap-profile1
Device(config-ap-profile)# dual-mode-ap-deployment-mode indoor
Device(config-ap-profile)# end
```

eap-method

To configure the Extensible Authentication Protocol (EAP) method for a Network Access Identifier (NAI) realm, use the **eap-method** command. To remove the EAP method for an NAI realm, use the **no** form of this command.

eap-method {**eap-aka** | **eap-fast** | **eap-leap** | **eap-peap** | **eap-sim** | **eap-tls** | **eap-ttls**}

Syntax Description

eap-aka	Enables EAP authentication and key agreement method. EAP-AKA is an EAP mechanism for authentication and session key distribution using the UMTS Subscriber Identity Module.
eap-fast	Enables EAP flexible authentication through the secure tunneling method. EAP-FAST is a flexible EAP protocol that allows mutual authentication of a supplicant and a server. It is similar to EAP-PEAP, but typically does not require the use of client or server certificates.
eap-leap	Enables EAP lightweight extensible authentication protocol method. EAP-LEAP is an EAP authentication protocol used primarily in Cisco Aironet WLANs. It encrypts data transmissions using dynamically generated wired equivalent privacy (WEP) keys, and supports mutual authentication.
eap-peap	Enables EAP-protected extensible authentication protocol method. EAP-PEAP is an EAP authentication protocol used in wireless networks and point-to-point connections. PEAP is designed to provide more secure authentication for 802.11 WLANs that support 802.1X port access control.
eap-sim	Enables EAP subscriber identity module method. EAP-SIM is an EAP authentication protocol used for authentication and session key distribution using the subscriber identity module (SIM) from the Global System for Mobile Communications (GSM).
eap-tls	Enables EAP transport layer security method. EAP-TLS is an EAP authentication protocol, and an IETF open standard that uses the Transport Layer Security (TLS) protocol. EAP-TLS is the original, standard wireless LAN EAP authentication protocol.
eap-ttls	Enables EAP-tunneled transport layer security method. EAP-TTLS is a simple WPA2-Enterprise Wi-Fi authentication method that has been a standard system for many years. When a user wants to connect to the network, the device initiates communication with the network and confirms that it is the correct network by identifying the server certificate.

Command Default

None

Command Modes

ANQP NAI EAP Configuration (config-anqp-nai-eap)

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.3.1	This command was introduced.

Example

The following example shows how to configure a EAP method:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless hotspot anqp-server my_anqp
Device(config-wireless-anqp-server)# nai-realm myvenue.cisco.com
Device(config-anqp-nai-eap)# eap-method eap-aka
```

eap profile

To configure an EAP profile, use the **eap profile** command.

eap profile *profile-name*

Syntax Description

profile-name	Name of the EAP profile. Maximum number of allowed characters is 63.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure an EAP profile name:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# eap profile eap-profile-name
```

et-analytics

To enable Encrypted Traffic Analytics (ETA) globally on Cisco Elastic Wireless LAN Controller (eWLC), use the **et-analytics** command.

et-analytics

Command Default None

Command Modes ET-Analytics configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

This example shows how to enable Encrypted Traffic Analytics (ETA) globally on Cisco Elastic Wireless LAN Controller (eWLC) in the ET-Analytics configuration mode:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# et-analytics
Device(config-et-analytics)# end
```

ethernet-vlan-transparent (mesh)

To configure ethernet bridging VLAN transparency for a mesh AP profile, use the **ethernet-vlan-transparent** command.

ethernet-vlan-transparent

Syntax Description

This command has no keywords or arguments.

Command Default

Ethernet bridging VLAN transparency is enabled.

Command Modes

config-wireless-mesh-profile

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Example

The following example shows how to configure ethernet bridging VLAN transparency for a mesh AP profile:

```
Device # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device (config)# wireless profile mesh mesh-profile
Device (config-wireless-mesh-profile)# ethernet-vlan-transparent
```

ethernet-bridging (mesh)

To configure ethernet bridging for a mesh AP profile, use the **ethernet-bridging** command.

ethernet-bridging

Syntax Description

This command has no keywords or arguments.

Command Default

Ethernet bridging is disabled.

Command Modes

config-wireless-mesh-profile

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Example

The following example shows how to configure ethernet bridging for a mesh AP profile:

```
Device # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device (config)# wireless profile mesh mesh-profile
Device (config-wireless-mesh-profile)# ethernet-bridging
```

event identity-update

To specify the match criteria to a policy map, use the **event identity-update** command.

event identity-update[**match-all** | **match-first**]

Syntax Description

match-all	Evaluates all the classes.
match-first	Evaluates the first class.

Command Default

None

Command Modes

config-event-control-policymap

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to specify the match criteria as match all classes to a policy map:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# policy-map type control subscriber policy-map-name
Device(config-event-control-policymap)# event identity-update match-all
```

exclusionlist

To configure an exclusion list, use the **exclusionlist** command. To disable an exclusion list, use the **no** form of this command.

exclusionlist [**timeout** *seconds*]
no exclusionlist [**timeout**]

Syntax Description

timeout *seconds*	(Optional) Specifies an exclusion list timeout in seconds. The range is from 0 to 2147483647. A value of zero (0) specifies no timeout.

Command Default

The exclusion list is set to 60 seconds.

Command Modes

Wireless policy configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

This example shows how to configure a client exclusion list:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy default-policy-profile
Device(config-wireless-policy)# exclusionlist timeout 5
```

exec-character-bits

To configure the character widths of EXEC and configuration command characters, use the **exec-character-bits** command in line configuration mode. To restore the default value, use the **no** form of this command.

exec-character-bits { *7* | *8* }

no exec-character-bits

Syntax Description

7	Sets the 7-bit character set. This is the default.
8	Sets the full 8-bit character set for use of international and graphical characters in banner messages, prompts, and so on.

Command Default

7-bit ASCII character set.

Command Modes

Line configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Usage Guidelines

Setting the EXEC character width to 8 allows you to use special graphical and international characters in banners, prompts, and so on. However, setting the EXEC character width to 8 bits can cause failures. For example, if a user on a terminal that is sending parity enters the **help** command, an "unrecognized command" message appears because the system is reading all 8 bits, and the eighth bit is not needed for the **help** command.

Examples

The following example shows how to configure the character widths of EXEC and configuration command characters :

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# line console 0
Device(config-line)# exec-character-bit 8
```

exec time-out

To set the interval that the EXEC command interpreter waits until user input is detected, use the **exec-timeout** command in line configuration mode. To remove the timeout duration, use the **no** form of this command.

exec time-out *minutes* [*seconds*]

exec time-out

Syntax Description

minutes	Integer that specifies the number of minutes. The default is 10 minutes.
seconds	(Optional) Additional time intervals, in seconds.

Command Default

10 minutes

Command Modes

Line configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Usage Guidelines

If no input is detected during the interval, the EXEC facility resumes the current connection. If no connections exist, the EXEC facility returns the terminal to the idle state and disconnects the incoming session.

To specify no timeout, enter the **exec-timeout 0 0** command.

Examples

The following example sets a time interval of 2 minutes, 30 seconds:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# line console 0
Device(config-line)# exec-timeout 12 0
```

exporter default-flow-exporter

To add an exporter to use to export records, use the **exporter default-flow-exporter** command. Use the **no** form of this command to disable the feature.

exporter default-flow-exporter

[no] exporter default-flow-exporter

Syntax Description

There are no arguments to this command.

Command Default

None

Command Modes

Flow monitor configuration

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.2.1	This command was introduced.

Example

This example shows how to add an exporter to use to export records:

```
Device(config-flow-monitor)#exporter default-flow-exporter
```

fabric control-plane

To configure the fabric control plane details, use the **fabric control-plane** command.

fabric control-plane *map-server-name*

Syntax Description

map-server-name	Refers to the fabric control plane name associated with the site tag.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

This example shows how to configure the fabric control plane details:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless tag site default-site-tag
Device(config-site-tag)# fabric control-plane
map-server-name
Device(config-site-tag)# end
```

factory-reset all

To delete rommon variables and start up config. To write 0s in all bootflash and harddisk partitions.

factory-reset all

Syntax Description

If the controller runs an image from bootflash, a copy is taken and restored to bootflash after disk partitions are zeroed.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 17.14.1	This command is introduced.

Usage Guidelines

You need to ensure the following:

- All the software images, configurations, and personal data are backed up.
- There is an uninterrupted power supply when the factory reset is in progress.
- Take a backup of the current image (especially if the current image the controller is running is not an image from bootflash).

Example

The following example shows how to delete rommon variables and start up config, also how to write 0s in all bootflash and harddisk partitions:

```
Device# factory-reset all
```

factory-reset all secure

To erase all user data and metadata from bootflash, use the **factory-reset all secure** command.

factory-reset all secure

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 17.14.1	This command is introduced.

Usage Guidelines

You need to boot a new image from TFTP post the secure erase as the image gets deleted. The erase takes around 5 to10 minutes. The erase is compliant with the National Institute of Standards and Technology (NIST) standards.

Example

The following example shows how to erase all user data and metadata from bootflash:

```
Device# factory-reset all secure
```

fast-teardown

To enable fast teardown for a mesh access point (AP) profile and configure the feature's parameters, use the **fast-teardown** command.

Note Fast Teardown for Mesh APs is not supported on Cisco Industrial Wireless (IW) 3702 Access Points.

fast-teardown {enabled | interval *duration* **latency-exceeded-threshold | latency-threshold | uplink-recovery-interval** *duration* **| retries** *retry limit*

Syntax Description

enabled	Enables the fast teardown feature.
interval	(optional) Configures the retry interval, in seconds. The valid values range between 1 and 10 seconds.
latency-exceeded-threshold	(optional) Specifies the latency interval in which at least one ping must succeed in less than threshold time. The valid values range between 1 and 30 seconds.
latency-threshold	(optional) Speficies the latency threshold. The valid values range between 1 and 500 milliseconds.
uplink-recovery-interval	(Optional) Specifies the time during which root acccess point uplink has to be stable to accept child connections. The valid values range between 1 and 3600 seconds.
retries	(optional) Specifies the maximum retries until the gateway is considered unreachable. The range is from 0 to 10.

Command Default

None

Command Modes

Fast Teardown configuration

Command History

Release	Modification
Cisco IOS XE Cupertino 17.7.1	This command was introduced.

Examples

The following example shows how to enable the fast teardown feature for a mesh AP profile and configure its parameters:

```
Device# configure terminal
Device(config)# wireless mesh profile mesh-profile-name
Device(config-wireless-mesh-profile)# fast-teardown
Device(config-wireless-mesh-profile-fast-teardown)# interval 1
```

fallback-radio-shut

To configure shutdown of the radio interface, use the **fallback-radio-shut** command.

fallback-radio-shut

Command Default None

Command Modes config-wireless-flex-profile

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure shutdown of the radio interface:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile flex flex-profile-name
Device(config-wireless-flex-profile)# fallback-radio-shut
```

fips authorization-key

To configure FIPS, use the **fips authorization-key** command.

fips authorization-key *key*

Syntax Description

key	The key length should be of 32 hexadecimal characters.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

Note Ensure that both the active and standby controllers have the same FIPS authorization key.

This example shows how to configure FIPS:

```
Device# configure terminal
Device(config)# fips authorization-key 12345678901234567890123456789012
Device(config)# end
```

flex

To configure flex related parameters, use the **flex** command.

flex {**nat-pat** | **split-mac-acl** *split-mac-acl-name* | **vlan-central-switching** }

Syntax Description

nat-pat	Enables NAT-PAT.
split-mac-acl	Configures split-mac-acl name.
split-mac-acl-name	Name of split MAC ACL.
vlan-central-switching	VLAN based central switching.

Command Default

None

Command Modes

config-wireless-policy

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

Examples

The following example shows how to configure flex related VLAN central-switching:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy profile-name
Device(config-wireless-policy)# flex vlan-central-switching
```

flow exporter

To create a flow exporter, or to modify an existing flow exporter, and enter flow exporter configuration mode, use the **flow exporter** command in global configuration mode. To remove a flow exporter, use the **no** form of this command.

flow exporter *exporter-name*
no flow exporter *exporter-name*

Syntax Description

exporter-name	Name of the flow exporter that is being created or modified.

Command Default

flow exporters are not present in the configuration.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

Flow exporters export the data in the flow monitor cache to a remote system, such as a server running NetFlow collector, for analysis and storage. Flow exporters are created as separate entities in the configuration. Flow exporters are assigned to flow monitors to provide data export capability for the flow monitors. You can create several flow exporters and assign them to one or more flow monitors to provide several export destinations. You can create one flow exporter and apply it to several flow monitors.

Examples

The following example creates a flow exporter named FLOW-EXPORTER-1 and enters flow exporter configuration mode:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)#
```

flow monitor

To create a flow monitor, or to modify an existing flow monitor, and enter flow monitor configuration mode, use the **flow monitor** command in global configuration mode. To remove a flow monitor, use the **no** form of this command.

flow monitor *monitor-name*
no flow monitor *monitor-name*

Syntax Description

monitor-name	Name of the flow monitor that is being created or modified.

Command Default

flow monitors are not present in the configuration.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

Flow monitors are the component that is applied to interfaces to perform network traffic monitoring. Flow monitors consist of a flow record and a cache. You add the record to the flow monitor after you create the flow monitor. The flow monitor cache is automatically created at the time the flow monitor is applied to the first interface. Flow data is collected from the network traffic during the monitoring process based on the key and nonkey fields in the flow monitor's record and stored in the flow monitor cache.

Examples

The following example creates a flow monitor named FLOW-MONITOR-1 and enters flow monitor configuration mode:

```
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)#
```

flow record

To create a flow record, or to modify an existing flow record, and enter flow record configuration mode, use the **flow record** command in global configuration mode. To remove a record, use the **no** form of this command.

flow record *record-name*
no flow record *record-name*

Syntax Description

record-name	Name of the flow record that is being created or modified.

Command Default

A flow record is not configured.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

A flow record defines the keys that uses to identify packets in the flow, as well as other fields of interest that gathers for the flow. You can define a flow record with any combination of keys and fields of interest. The supports a rich set of keys. A flow record also defines the types of counters gathered per flow. You can configure 64-bit packet or byte counters.

Examples

The following example creates a flow record named FLOW-RECORD-1, and enters flow record configuration mode:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)#
```

full-sector-dfs (mesh)

To configure mesh full sector Dynamic Frequency Selection (DFS) status for a mesh AP profile, use the **full-sector-dfs** command.

full-sector-dfs

Syntax Description

This command has no keywords or arguments.

Command Default

Full sector DFS is enabled.

Command Modes

config-wireless-mesh-profile

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Example

The following example shows how to configure mesh full sector DFS status for a mesh AP profile:

```
Device # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device (config)# wireless profile mesh mesh-profile
Device (config-wireless-mesh-profile)# full-sector-dfs
```