Configuration Commands: g to z

- gas-ap-rate-limit, on page 8
- group, on page 9
- gtk-randomize, on page 10
- hessid , on page 11
- hotspot anqp-server, on page 12
- icon, on page 13
- idle-timeout , on page 14
- image-download-mode , on page 15
- inactive-timeout, on page 16
- install add profile default, on page 17
- install activate, on page 19
- install activate auto-abort-timer, on page 20
- install activate file, on page 21
- install commit, on page 22
- install remove profile default , on page 23
- install deactivate , on page 24
- install rollback, on page 25
- interface vlan, on page 26
- ip access-group, on page 27
- ip access-list extended , on page 28
- ip address, on page 29
- ip dhcp pool, on page 31
- ip dhcp-relay information option server-override, on page 33
- ip dhcp-relay source-interface, on page 35
- ip domain lookup, on page 36
- ip domain-name , on page 38
- ip flow-export destination, on page 39
- ip helper-address, on page 40
- ip http authentication, on page 43
- ip http auth-retry, on page 45
- ip http active-session-modules, on page 46
- ip http client secure-ciphersuite, on page 47
- ip http secure-ciphersuite, on page 48

- ip http secure-server, on page 50
- ip http server, on page 52
- ip http session-module-list, on page 54
- ip ssh, on page 56
- ip ssh version, on page 58
- ip tftp blocksize, on page 60
- ip verify source, on page 61
- ipv4-address-type, on page 62
- ipv4 dhcp , on page 63
- ipv4 flow monitor , on page 64
- ipv6 access-list, on page 65
- ipv6-address-type, on page 67
- ipv6 address, on page 68
- ipv6 dhcp pool, on page 70
- ipv6 enable, on page 73
- ipv6 mld snooping, on page 75
- ipv6 nd managed-config-flag , on page 76
- ipv6 nd other-config-flag , on page 77
- ipv6 nd ra throttler attach-policy , on page 78
- ipv6 nd raguard policy, on page 79
- ipv6 traffic-filter , on page 81
- key chain, on page 82
- key config-key, on page 83
- **key config-key password-encrypt**, on page 84
- license air level, on page 85
- license smart (global config), on page 87
- license smart (privileged EXEC), on page 98
- line vty , on page 104
- local-auth ap eap-fast , on page 105
- local-site , on page 106
- location expiry , on page 107
- location notify-threshold, on page 108
- log-export-mode , on page 109
- login authentication , on page 110
- login block-for, on page 111
- mac-filtering , on page 112
- mab request format attribute, on page 113
- mbo, on page 115
- match (access-map configuration), on page 116
- match activated-service-template, on page 118
- match any , on page 120
- match day, on page 121
- match device-type, on page 122
- match eap-type, on page 123
- match join-time-of-day, on page 124
- match message-type, on page 125

- match non-client-nrt, on page 126
- match protocol, on page 127
- match service-instance, on page 130
- match service-type, on page 131
- match user-role , on page 132
- match username, on page 133
- match (access-map configuration), on page 134
- match (class-map configuration), on page 136
- match wlan user-priority, on page 139
- max-bandwidth , on page 140
- max-through, on page 141
- mdns-sd, on page 142
- mdns-sd flex-profile, on page 143
- mdns-sd profile, on page 144
- method, on page 145
- method fast , on page 146
- mgmtuser username , on page 147
- mobility backhaul-check coordinator-down, on page 148
- mobility backhaul-check eth-down , on page 149
- mobility mpo cos, on page 150
- mobility mpo enable, on page 151
- mobility mpo path, on page 152
- mobility mpo rssi , on page 153
- mobility mpo telemetry, on page 154
- mobility role, on page 155
- mobility scan , on page 156
- monitor capture (access list/class map), on page 157
- monitor capture export, on page 159
- monitor capture (interface/control plane), on page 160
- monitor capture limit, on page 161
- monitor capture match, on page 163
- monitor capture start, on page 166
- monitor capture stop, on page 167
- mop sysid, on page 168
- mpls ether-filter ethernet-I, on page 169
- mpls ether-filter ethertypes filtering, on page 170
- mpls high-availability timeout, on page 171
- multicast (URWB), on page 172
- multicast vlan, on page 173
- name, on page 174
- nac, on page 175
- nai-realm, on page 176
- nai-realm (OSU Provider), on page 177
- nas-id option2 , on page 178
- network , on page 179
- network-key key, on page 180

- network-type, on page 181
- nmsp cloud-services enable , on page 182
- nmsp cloud-services http-proxy , on page 183
- nmsp cloud-services server token , on page 184
- nmsp cloud-services server url, on page 185
- nmsp notification interval, on page 186
- nmsp strong-cipher, on page 188
- no shutdown (URWB), on page 189
- operator, on page 190
- operating-class, on page 191
- option, on page 192
- osu-provider, on page 194
- osu-ssid, on page 195
- parameter-map type subscriber attribute-to-service , on page 196
- parameter-map type webauth , on page 197
- password encryption aes, on page 198
- peer-blocking, on page 199
- policy, on page 200
- police, on page 201
- police cir, on page 203
- policy-map, on page 204
- policy-map, on page 206
- port, on page 208
- priority priority-value, on page 209
- public-ip, on page 210
- qos-map, on page 211
- qos video, on page 214
- radius server, on page 215
- radius-server deadtime, on page 216
- radius-server attribute wireless accounting call-station-id, on page 217
- radius-server attribute wireless authentication call-station-id, on page 219
- range, on page 221
- record wireless avc basic, on page 222
- redirect , on page 223
- redirect portal , on page 224
- remote-lan, on page 225
- rf tag, on page 226
- roaming-oi, on page 227
- rrc-evaluation, on page 228
- security , on page 229
- security dot1x authentication-list, on page 230
- security ft, on page 231
- security pmf, on page 233
- security static-wep-key , on page 235
- security web-auth, on page 236
- security wpa akm, on page 237

- server-uri, on page 239
- service-policy, on page 240
- service-policy qos , on page 241
- service-template, on page 242
- service timestamps, on page 243
- session-timeout, on page 245
- set, on page 246
- sftp-image-path (image-download-mode sftp), on page 253
- sftp-image-server (image-download-mode sftp), on page 254
- sftp-password (image-download-mode sftp), on page 255
- sftp-password (trace-export), on page 256
- sftp-path, on page 257
- sftp-server, on page 258
- sftp-username (image-download-mode sftp), on page 259
- sftp-username (trace-export), on page 260
- snmp-server enable traps wireless, on page 261
- snmp-server group, on page 262
- snmp-server subagent cache, on page 265
- ssid broadcast persistent, on page 266
- stopbits, on page 267
- strong-network-key, on page 268
- tag rf, on page 269
- tag site, on page 270
- tftp-image-path (image-download-mode tftp), on page 271
- tftp-image-server (image-download-mode tftp), on page 272
- tftp-path, on page 273
- tftp-server, on page 274
- udp-timeout, on page 275
- umbrella-param-map, on page 276
- update-timer, on page 277
- urwb chan-list channel, on page 278
- urwb channel, on page 279
- urwb crypto policy, on page 280
- urwb crypto rotating-key-timeout, on page 281
- urwb cwidth , on page 282
- urwb-profile, on page 283
- urwb ptmp autoscan, on page 284
- urwb ptmp cluster-id, on page 285
- urwb ptmp rssi-threshold, on page 286
- urwb ptmp tower-id, on page 287
- urwb role, on page 288
- username, on page 289
- venue, on page 291
- violation, on page 292
- wan-metrics, on page 293
- wgb broadcast-tagging, on page 294

- wgb vlan, on page 295
- whitelist acl, on page 296
- wired-vlan-range, on page 297
- config wlan assisted-roaming, on page 298
- wireless aaa policy, on page 299
- wireless aaa policy, on page 300
- wireless autoqos policy-profile , on page 301
- wireless broadcast vlan, on page 302
- wireless client, on page 303
- wireless client mac-address, on page 305
- wireless client vlan-persistent, on page 310
- wireless config validate , on page 311
- wireless country, on page 313
- wireless exclusionlist mac address, on page 314
- wireless hotspot anqp-server, on page 315
- wireless hotspot gas-rate-limit, on page 316
- wireless hotspot icon, on page 317
- wireless ipv6 ra wired, on page 318
- wireless load-balancing, on page 319
- wireless macro-micro steering transition-threshold , on page 320
- wireless macro-micro steering probe-suppression, on page 321
- wireless management certificate, on page 322
- wireless management interface, on page 323
- wireless management trustpoint, on page 324
- wireless ewc-ap ap ap-type, on page 325
- wireless ewc-ap ap capwap, on page 326
- wireless ewc-ap ap reload, on page 327
- wireless ewc-ap ap shell , on page 328
- wireless ewc-ap ap shell username, on page 329
- wireless ewc-ap preferred-master, on page 330
- wireless ewc-ap factory-reset, on page 331
- wireless ewc-ap vrrp vrid, on page 332
- wireless profile calender-profile name, on page 333
- wireless profile image-download default, on page 334
- wireless profile policy, on page 335
- wireless profile transfer, on page 336
- wireless profile urwb, on page 337
- wireless rfid, on page 338
- wireless security dot1x, on page 339
- wireless security dot1x radius accounting mac-delimiter, on page 341
- wireless security dot1x radius accounting username-delimiter, on page 342
- wireless security dot1x radius callStationIdCase, on page 343
- wireless security dot1x radius mac-authentication call-station-id, on page 344
- wireless security dot1x radius mac-authentication mac-delimiter, on page 345
- wireless security web-auth retries, on page 346
- wireless tag policy, on page 347

- wireless tag site, on page 348
- wireless wps ap-authentication threshold, on page 349
- wireless wps client-exclusion, on page 350
- wireless wps mfp, on page 352
- wireless wps mfp ap-impersonation, on page 353
- wireless wps rogue network-assurance enable, on page 354
- wireless wps rogue ap aaa , on page 355
- wireless wps rogue ap aaa polling-interval, on page 356
- wireless wps rogue ap init-timer, on page 357
- wireless wps rogue ap mac-address rldp initiate , on page 358
- wireless wps rogue ap notify-min-rssi, on page 359
- wireless wps rogue ap notify-rssi-deviation, on page 360
- wireless wps rogue ap rldp alarm-only, on page 361
- wireless wps rogue ap rldp alarm-only monitor-ap-only, on page 362
- wireless wps rogue ap rldp auto-contain, on page 363
- wireless wps rogue ap rldp retries, on page 364
- wireless wps rogue ap rldp schedule, on page 365
- wireless wps rogue ap rldp schedule day, on page 366
- wireless wps rogue ap timeout, on page 367
- wireless wps rogue auto-contain , on page 368
- wireless wps rogue client aaa, on page 369
- wireless wps rogue client mse, on page 370
- wireless wps rogue client client-threshold , on page 371
- wireless wps rogue client notify-min-rssi, on page 372
- wireless wps rogue client notify-rssi-deviation, on page 373
- wireless wps rogue rule, on page 374
- wireless wps rogue security-level, on page 376
- wireless-default radius server, on page 377
- wlan policy , on page 378

gas-ap-rate-limit

To set the number of Generic Advertisement Service (GAS) or Access Network Query Protocol (ANQP) request action frames sent to the controller by an access point (AP) for a given duration, use the **gas-ap-rate-limit** command.

gas-ap-rate-limit *number-of-requests request-limit-interval*

Syntax Description

number-of-requests	Number of GAS or ANQP requests allowed in a given interval. Valid range is from 1-100.
request-limit-interval	Interval in which the maximum numbers of requests is applicable. Valid range is from 100-1000 milliseconds.

Command Default

Limit is not enabled.

Command Modes

AP Profile Configuration (config-ap-profile)

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 GAS or ANQP request action frames sent to the controller by an AP for a given duration:

```
Device(config)# ap profile hotspot
Device(config-ap-profile)# gas-ap-rate-limit 12 120
```

group

To configure a group for a venue and a venue type, use the **group** command. To remove the group, use the **no** form of the command.

group *venue-group venue-type*

Syntax Description

venue-group	Venue group. Options are: **assembly**, **business**, **educational**, **industrial**, **institutional**, **mercantile**, **outdoor**, **residential**, **storage**, **unspecified**, **utility**, and **vehicular**.
venue-type	Venue type. The options vary based on the venue-group.

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 group for a venue and a venue type:

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# group business bank
```

gtk-randomize

To configure random-GTK for hole-196 mitigation, use the **gtk-randomize** command. Use the **no** form of the command to remove the icon.

gtk-randomize

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 Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

The GTK used for each mobile device should be different from every GTK used for the other mobile devices associated to the BSS.

Example

The following example shows how to configure random-GTK for hole-196 mitigation.

```
Device(config-wlan)# security wpa wpa2 gtk-randomize
```

hessid

To configure a homogenous extended service set, use the **hessid** command. To remove the service set, use the **no** form of the command.

hessid *HESSID-value*

Syntax Description

HESSID-value	HESSID value.

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 homogenous extended service set:

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# hessid 00:40:96:b4:82:55
```

hotspot anqp-server

To associate a hotspot server with a policy profile, use the **hotspot anqp-server** command. To remove the server, use the **no** form of the command.

hotspot anqp-server *server-name*

Syntax Description

server-name	Name of the Hotspot 2.0 ANQP server.

Command Default

None

Command Modes

Wireless Policy Configuration (config-wireless-policy)

Command History

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

Example

The following example shows how to configure a Hotspot 2.0 ANQP server:

```
Device(config)# wireless profile policy hs-policy
Device(config-wireless-policy)# hotspot anqp-server test
```

icon

To configure an icon for an Online Sign-Up (OSU) provider, use the **icon** command. To remove the icon, use the **no** form of the command.

icon *file-name*

Syntax Description

file-name	File name of the icon.

Command Default

None

Command Modes

ANQP OSU Provider Configuration (config-anqp-osu-provider)

Command History

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

Usage Guidelines

The icon must be configured under the hotspot ANQP server.

Example

The following example shows how to configure an icon for the OSU provider:

```
Device(config-wireless-anqp-server)# osu-provider my-osu
Device(config-anqp-osu-provider)# icon test
```

idle-timeout

To configure the idle-timeout value in seconds for a wireless profile policy, use the **idle-timeout** command.

idle-timeout *value*

Syntax Description

value	Sets the idle-timeout value. Valid range is 15 to 100000 seconds.

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 set the idle-timeout in a wireless profile policy:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy policy-profile-name
Device(config-wireless-policy)# idle-timeout 100
```

image-download-mode

To configure image download using the HTTP, SFTP, TFTP, or CCO modes, use the **image-download-mode** command.

image-download-mode { **http** | **sftp** | **tftp** | **cco** }

Syntax Description

http	Configures image download using the HTTP mode.
sftp	Configures image download using the SFTP mode.
tftp	Configures image download using the TFTP mode.
cco	Configures image download using the CCO mode.

Command Default

None

Command Modes

Wireless image download profile configuration mode

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.
Cisco IOS XE Amsterdam 17.1.1s	The **image-download-mode cco**was introduced.

Example

```
Device(config)# wireless profile image-download default
Device(config-wireless-image-download-profile)# image-download-mode http
```

inactive-timeout

To enable in-active timer, use the **inactive-timeout** command.

inactive-timeout *timeout-in-seconds*

Syntax Description

timeout-in-seconds	Specifies the inactive flow timeout value. The range is from 1 to 604800.

Command Default

None

Command Modes

ET-Analytics configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1 Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

This example shows how to enable in-active timer 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)# inactive-timeout 15
Device(config-et-analytics)# end
```

install add profile default

To download the embedded wireless controller image from the external server, use the **install add profile default** command.

install add profile *profile_name***activatecommitprompt-level none**

Syntax Description

add	Installs a package file to the system.
profile	Selects a profile.
profile_name	Adds a profile name with a maximum of 15 characters. Specify **default** to trigger the default behaviour.
activate	Activates the installed profile.
commit	Commits the changes to the loadpath.
prompt-level	Sets the prompt-level to none.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Usage Guidelines

Ensure that you have the *image-download-profile* configured on embedded wireless controller. Extract the contents of the image bundle (.zip archive) to an external TFTP or HTTP(S) server. The .zip archive contains the controller image and various compatible AP images (`apXgY`).

Example

The following example shows how to download the embedded wireless controller image:

```
Device#install add profile default

install_add: START Thu Jan 24 20:08:01 UTC 2019
Jan 24 20:08:03.389: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
add
Jan 24 20:08:03.389 %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
add
install_add: Default profile addition successful
SUCCESS: install_add Thu Jan 24 20:08:03 UTC 2019
Jan 24 20:08:04.358: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install add
Jan 24 20:08:04.358 %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install add
WLC#
*Jan 24 20:08:03.350: %INSTALL-5-INSTALL_START_INFO: Chassis 1 R0/0: install_engine: Started
 install add
```

```
*Jan 24 20:08:04.335: %INSTALL-5-INSTALL_COMPLETED_INFO: Chassis 1 R0/0: install_engine:
Completed install add
```

Note The log `Completed install add` means that the command is successful and the download will start soon.

The following example verifies the the image download status:

```
Device#sh wireless ewc-ap predownload status
```

install activate

To activate an installed package, use the **install activate** command.

install activate {**auto-abort-timer** | **file** | **profile** | **prompt-level**}

Syntax Description

auto-abort-timer	Sets the cancel timer. The time range is between 30 and 1200 minutes.
file	Specifies the package to be activated.
profile	Specifies the profile to be activated.
prompt-level	Sets the prompt level.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

The following example shows how to activate the installed package:

```
Device# install activate profile default
install_activate: START Thu Nov 24 20:14:53 UTC 2019

System configuration has been modified.
Press Yes(y) to save the configuration and proceed.
Press No(n) for proceeding without saving the configuration.
Press Quit(q) to exit, you may save configuration and re-enter the command. [y/n/q] y
Building configuration...
[OK]Modified configuration has been saved
Jan 24 20:15:02.745: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
activate
Jan 24 20:15:02.745 %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
activate
install_activate: Activating PACKAGE
```

install activate auto-abort-timer

To set the abort timer, use the **install activate auto-abort-timer** command.

install activate auto-abort-timer *<30-1200>* **prompt-level none**

Syntax Description

auto-abort-timer	Sets the cancel timer. The time range is between 30 and 1200 minutes.
<30-1200>	Specifies the cancel timer time in minutes.
prompt-level	Specifies the prompt level.
none	Specifies no prompting.

Command Default

None

Command Modes

Privileged EXEC (#)

Task ID

Task ID	Operation
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

The following example shows how to activate the cancel timer:

```
Device#install activate auto-abort-timer 30 prompt-level none
```

install activate file

To activate an installed package, use the **install activate file** command.

install activate file *file-name*

Syntax Description

file-name	Specifies the package name. Options are: bootflash:, flash:, and webui:.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

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

Example

The following example shows how to use an auto cancel timer while activating an install package on a standby location:

```
Device# install activate file vwlc_apsp_16.11.1.0_74.bin
```

install commit

To commit the changes to the loadpath, use the **install commit** command.

install commit

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

The following example shows how to commit the changes to the loadpath:

```
Device# install commit
```

install remove profile default

To specify an install package that is to be removed, use the **install remove profile default** command.

install remove profile default

Syntax Description

remove	Removes the install package.
profile	Specifies the profile to be removed.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

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

Example

The following example shows how to remove a default profile:

```
Device# install remove profile default
```

install deactivate

To specify an install package that is to be deactivated, use the **install deactivate file** command.

install deactivate file *file-name*

Syntax Description

file-name	Specifies the package name. Options are: bootflash:, flash:, and webui:.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

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

Example

The following example shows how to deactivate an install package:

```
Device# install deactivate file vwlc_apsp_16.11.1.0_74.bin
```

install rollback

To roll back to a particular installation point, use the **install rollback** command.

install rollback to {**base** | **committed** | **id** *id* | **label** *label*} [**prompt-level none**]

Syntax Description

base	Rolls back to the base image.
prompt-level none	Sets the prompt level as none.
committed	Rolls back to the last committed installation point.
id	Rolls back to a specific install point ID.
label	Rolls back to a specific install point label.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

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

Example

The following example shows how to specify the ID of the install point to roll back to:

```
Device# install rollback to id 1
```

interface vlan

To create or access a dynamic switch virtual interface (SVI) and to enter interface configuration mode, use the **interface vlan** command in global configuration mode. To delete an SVI, use the **no** form of this command.

interface vlan *vlan-id*
no interface vlan *vlan-id*

Syntax Description

vlan-id	VLAN number. The range is 1 to 4094.

Command Default

The default VLAN interface is VLAN 1.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1 Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

SVIs are created the first time you enter the **interface vlan** *vlan-id* command for a particular VLAN. The *vlan-id* corresponds to the VLAN-tag associated with data frames on an IEEE 802.1Q encapsulated trunk or the VLAN ID configured for an access port.

Note When you create an SVI, it does not become active until it is associated with a physical port.

If you delete an SVI using the **no interface vlan** *vlan-id* command, it is no longer visible in the output from the **show interfaces** privileged EXEC command.

Note You cannot delete the VLAN 1 interface.

You can reinstate a deleted SVI by entering the **interface vlan** *vlan-id* command for the deleted interface. The interface comes back up, but the previous configuration is gone.

The interrelationship between the number of SVIs configured on a chassis or a chassis stack and the number of other features being configured might have an impact on CPU utilization due to hardware limitations. You can use the **sdm prefer** global configuration command to reallocate system hardware resources based on templates and feature tables.

You can verify your setting by entering the **show interfaces** and **show interfaces vlan** *vlan-id* privileged EXEC commands.

This example shows how to create a new SVI with VLAN ID 23 and enter interface configuration mode:

```
Device(config)# interface vlan 23
Device(config-if)#
```

ip access-group

To configure WLAN access control group (ACL), use the **ip access-group** command. To remove a WLAN ACL group, use the **no** form of the command.

ip access-group [**web**] *acl-name*
no ip access-group [**web**]

Syntax Description

web	(Optional) Configures the IPv4 web ACL.
acl-name	Specify the preauth ACL used for the WLAN with the security type value as webauth.

Command Default

None

Command Modes

WLAN configuration

Usage Guidelines

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

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
Cisco IOS XE Gibraltar 16.12.1	

This example shows how to configure a WLAN ACL:

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#wlan wlan1
Device(config-wlan)#ip access-group test-acl
```

This example shows how to configure an IPv4 WLAN web ACL:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# ip access-group web test
Device(config-wlan)#
```

ip access-list extended

To configure extended access list, use the **ip access-list extended** command.

ip access-list extended {**<100-199>** | **<2000-2699>** *access-list-name*}

Syntax Description

<100-199>	Extended IP access-list number.
<2000-2699>	Extended IP access-list number (expanded range).

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 extended access list:

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

ip address

To set a primary or secondary IP address for an interface, use the **ip address** command in interface configuration mode. To remove an IP address or disable IP processing, use the noform of this command.

ip address *ip-address mask* [**secondary** [**vrf** *vrf-name*]]
no ip address *ip-address mask* [**secondary** [**vrf** *vrf-name*]]

Syntax Description

ip-address	IP address.
mask	Mask for the associated IP subnet.
secondary	(Optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address. **Note** If the secondary address is used for a VRF table configuration with the **vrf** keyword, the **vrf** keyword must be specified also.
vrf	(Optional) Name of the VRF table. The *vrf-name* argument specifies the VRF name of the ingress interface.

Command Default

No IP address is defined for the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

An interface can have one primary IP address and multiple secondary IP addresses. Packets generated by the Cisco IOS software always use the primary IP address. Therefore, all devices and access servers on a segment should share the same primary network number.

Hosts can determine subnet masks using the Internet Control Message Protocol (ICMP) mask request message. Devices respond to this request with an ICMP mask reply message.

You can disable IP processing on a particular interface by removing its IP address with the **no ip address** command. If the software detects another host using one of its IP addresses, it will print an error message on the console.

The optional **secondary** keyword allows you to specify an unlimited number of secondary addresses. Secondary addresses are treated like primary addresses, except the system never generates datagrams other than routing updates with secondary source addresses. IP broadcasts and Address Resolution Protocol (ARP) requests are handled properly, as are interface routes in the IP routing table.

Secondary IP addresses can be used in a variety of situations. The following are the most common applications:

- There may not be enough host addresses for a particular network segment. For example, your subnetting allows up to 254 hosts per logical subnet, but on one physical subnet you need 300 host addresses. Using

secondary IP addresses on the devices or access servers allows you to have two logical subnets using one physical subnet.

- Many older networks were built using Level 2 bridges. The judicious use of secondary addresses can aid in the transition to a subnetted, device-based network. Devices on an older, bridged segment can be easily made aware that many subnets are on that segment.
- Two subnets of a single network might otherwise be separated by another network. This situation is not permitted when subnets are in use. In these instances, the first network is *extended*, or layered on top of the second network using secondary addresses.

Note

- If any device on a network segment uses a secondary address, all other devices on that same segment must also use a secondary address from the same network or subnet. Inconsistent use of secondary addresses on a network segment can very quickly cause routing loops.
- When you are routing using the Open Shortest Path First (OSPF) algorithm, ensure that all secondary addresses of an interface fall into the same OSPF area as the primary addresses.
- If you configure a secondary IP address, you must disable sending ICMP redirect messages by entering the **no ip redirects** command, to avoid high CPU utilization.

Examples

In the following example, 192.108.1.27 is the primary address and 192.31.7.17 is the secondary address for GigabitEthernet interface 1/0/1:

```
Device# enable
Device# configure terminal
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# ip address 192.108.1.27 255.255.255.0
Device(config-if)# ip address 192.31.7.17 255.255.255.0 secondary
```

Related Commands

Command	Description
match ip route-source	Specifies a source IP address to match to required route maps that have been set up based on VRF connected routes.
route-map	Defines the conditions for redistributing routes from one routing protocol into another, or to enable policy routing.
set vrf	Enables VPN VRF selection within a route map for policy-based routing VRF selection.
show ip arp	Displays the ARP cache, in which SLIP addresses appear as permanent ARP table entries.
show ip interface	Displays the usability status of interfaces configured for IP.
show route-map	Displays static and dynamic route maps.

ip dhcp pool

To configure a Dynamic Host Configuration Protocol (DHCP) address pool on a DHCP server and enter DHCP pool configuration mode, use the **ip dhcp pool** command in global configuration mode. To remove the address pool, use the no form of this command.

ip dhcp pool *name*
no ip dhcp pool *name*

Note When configuring the **ip dhcp pool** command, note that it can be affected by the **ip dhcp database** command if an incorrect URL is provided. The console may hang due to multiple attempts by the DHCP service to reach the URL before it returns a failure. This is expected behavior. To prevent this issue, ensure that the correct URL, including the file name, is provided when using the **ip dhcp database** command, especially when it includes ftp/tftp.

Syntax Description

name	Name of the pool. Can either be a symbolic string (such as engineering) or an integer (such as 0).

Command Default

DHCP address pools are not configured.

Command Modes

Global 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.

Usage Guidelines

During execution of this command, the configuration mode changes to DHCP pool configuration mode, which is identified by the (config-dhcp)# prompt. In this mode, the administrator can configure pool parameters, like the IP subnet number and default router list.

Examples

The following example configures pool1 as the DHCP address pool:

```
ip dhcp pool pool1
```

Related Commands

Command	Description
host	Specifies the IP address and network mask for a manual binding to a DHCP client.
ip dhcp excluded-address	Specifies IP addresses that a Cisco IOS DHCP server should not assign to DHCP clients.

Command	Description
network (DHCP)	Configures the subnet number and mask for a DHCP address pool on a Cisco IOS DHCP server.

ip dhcp-relay information option server-override

To enable the system to globally insert the server ID override and link selection suboptions into the DHCP relay agent information option in forwarded BOOTREQUEST messages to a Dynamic Host Configuration Protocol (DHCP) server, use the **ip dhcp-relay information option server-override** command in global configuration mode. To disable inserting the server ID override and link selection suboptions into the DHCP relay agent information option, use the **no** form of this command.

ip dhcp-relay information option server-override
no ip dhcp-relay information option server-override

Syntax Description

This command has no arguments or keywords.

Command Default

The server ID override and link selection suboptions are not inserted into the DHCP relay agent information option.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Aggregation Services Routers.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

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

The **ip dhcp-relay information option server-override** command adds the following suboptions into the relay agent information option when DHCP broadcasts are forwarded by the relay agent from clients to a DHCP server:

- Server ID override suboption
- Link selection suboption

When this command is configured, the gateway address (giaddr) will be set to the IP address of the outgoing interface, which is the interface that is reachable by the DHCP server.

If the **ip dhcp relay information option server-id-override** command is configured on an interface, it overrides the global configuration on that interface only.

Examples

In the following example, the DHCP relay will insert the server ID override and link selection suboptions into the relay information option of the DHCP packet. The loopback interface IP address is configured to be the source IP address for the relayed messages.

```
Device(config)# ip dhcp-relay information option server-override
Device(config)# ip dhcp-relay source-interface loopback 0
Device(config)# interface Loopback 0
Device(config-if)# ip address 10.2.2.1 255.255.255.0
```

Related Commands

Command	Description
ip dhcp relay information option server-id-override	Enables the system to insert the server ID override and link selection suboptions on a specific interface into the DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server.

ip dhcp-relay source-interface

To globally configure the source interface for the relay agent to use as the source IP address for relayed messages, use the **ip dhcp-relay source-interface** command in global configuration mode. To remove the source interface configuration, use the **no** form of this command.

ip dhcp-relay source-interface *type number*
no ip dhcp-relay source-interface *type number*

Syntax Description

type	Interface type. For more information, use the question mark (?) online help function.
number	Interface or subinterface number. For more information about the numbering system for your networking device, use the question mark (?) online help function.

Command Default

The source interface is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Aggregation Services Routers.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

The **ip dhcp-relay source-interface** command allows the network administrator to specify a stable, hardware-independent IP address (such as a loopback interface) for the relay agent to use as a source IP address for relayed messages.

If the **ip dhcp-relay source-interface** global configuration command is configured and the **ip dhcp relay source-interface** command is also configured, the **ip dhcp relay source-interface** command takes precedence over the global configuration command. However, the global configuration is applied to interfaces without the interface configuration.

Examples

In the following example, the loopback interface IP address is configured to be the source IP address for the relayed messages:

```
Device(config)# ip dhcp-relay source-interface loopback 0
Device(config)# interface loopback 0
Device(config-if)# ip address 10.2.2.1 255.255.255.0
```

Related Commands

Command	Description
ip dhcp relay source-interface	Configures the source interface for the relay agent to use as the source IP address for relayed messages.

ip domain lookup

To enable IP Domain Name System (DNS)-based hostname-to-address translation, use the **ip domain lookup** command in global configuration mode. To disable DNS-based hostname-to-address translation, use the **no** form of this command.

ip domain lookup [**nsap** | **recursive** | **source-interface** *interface-type-number* | **vrf** *vrf-name* { **source-interface** *interface-type-number* }]

Syntax Description

nsap	(Optional) Enables IP DNS queries for Connectionless Network Service (CLNS) and Network Service Access Point (NSAP) addresses.
recursive	(Optional) Enables IP DNS recursive lookup.
source-interface *interface-type-number*	(Optional) Specifies the source interface for the DNS resolver. Enter an interface type and number.
vrf *vrf-name*	(Optional) Defines a Virtual Routing and Forwarding (VRF) table. For vrf-name, enter a name for the VRF table.

Command Default

IP DNS-based hostname-to-address translation is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.
Cisco IOS XE Dublin 17.12.1	An issue relating to the configuration of the **ip domain lookup source-interface** *interface-type-number* command on Layer 3 physical interfaces was resolved. Starting from this release, even if configured on a Layer 3 physical interface, the command is retained across reloads and in case the port mode is changed.

Usage Guidelines

If this command is enabled on a device and you execute the **show tcp brief** command, the output may be displayed very slowly.

When both IP and ISO CLNS are enabled on a device, the **ip domain lookup nsap** command allows you to discover a CLNS address without having to specify a full CLNS address, given a hostname.

This command is useful for the **ping** (ISO CLNS) command, and for CLNS Telnet connections.

If you configure the **ip domain lookup source-interface** *interface-type-number* command on a Layer 3 physical interface, note the following: If the port mode is changed or in case of a device reload, the command is automatically removed from running configuration (Refer to the output of the **show running-configuration** privileged EXEC command when this happens). Removal of the command causes DNS queries that use the specified source interface, to be dropped. The only available workaround is to reconfigure the command. Starting with Cisco IOS XE Dublin 17.12.1, this issue is resolved.

Examples

The following example shows how to configure IP DNS-based hostname-to-address translation:

```
Device# configure terminal
Device(config)# ip domain lookup
Device(config)# end
```

The following example shows how to configure a source interface for the DNS domain lookup:

```
Device# configure terminal
Device(config)# ip domain lookup source-interface gigabitethernet1/0/2
Device(config)# end
```

ip domain-name

To configure the host domain on the device, use the **ip domain-name** command.

ip domain-name *domain-name* [**vrf** *vrf-name*]

Syntax Description

domain-name	Default domain name.
vrf-name	Specifies the virtual routing and forwarding (VRF) to use to resolve the domain name.

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 a host domain in a device:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ip domain-name domain-name
```

ip flow-export destination

To configure ETA flow export destination, use the **ip flow-export destination** command.

ip flow-export destination *ip_address port_number*

Syntax Description

port_number	Port number. The range is from 1 to 65535.

Command Default

None

Command Modes

ET-Analytics configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1 Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

This example shows how to configure ETA flow export destination 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)# ip flow-export
destination 120.0.0.1 2055
Device(config-et-analytics)# end
```

ip helper-address

To enable forwarding of User Datagram Protocol (UDP) broadcasts, including Bootstrap Protocol (BOOTP), received on an interface, use the **ip helper-address** command in interface configuration mode. To disable forwarding of broadcast packets to specific addresses, use the**no** form of this command.

ip helper-address[**vrf** *name* | **global**] *address* {[**redundancy** *vrg-name*]}
no ip helper-address [**vrf** *name* | **global**] *address* {[**redundancy** *vrg-name*]}

Syntax Description

vrf *name*	(Optional) Enables the VPN routing and forwarding (VRF) instance and the VRF name.
global	(Optional) Configures a global routing table.
address	Destination broadcast or host address to be used when forwarding UDP broadcasts. There can be more than one helper address per interface.
redundancy *vrg-name*	(Optional) Defines the Virtual Router Group (VRG) name.

Command Default

UDP broadcasts are not forwarded.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.0	This command was introduced.
12.2(4)B	This command was modified. The **vrf** *name* keyword and argument pair and the **global** keyword were added.
12.2(15)T	This command was modified. The **redundancy** *vrg-name* keyword and argument pair was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
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.

Usage Guidelines

The **ip forward-protocol** command along with the **ip helper-address** command allows you to control broadcast packets and protocols that are forwarded.

One common application that requires helper addresses is DHCP, which is defined in RFC 1531. To enable BOOTP or DHCP broadcast forwarding for a set of clients, configure a helper address on the router interface connected to the client. The helper address must specify the address of the BOOTP or DHCP server. If you have multiple servers, configure one helper address for each server.

The following conditions must be met for a UDP or IP packet to be able to use the **ip helper-address** command:

- The MAC address of the received frame must be all-ones broadcast address (ffff.ffff.ffff).

- The IP destination address must be one of the following: all-ones broadcast (255.255.255.255), subnet broadcast for the receiving interface, or major-net broadcast for the receiving interface if the **no ip classless** command is also configured.
- The IP time-to-live (TTL) value must be at least 2.
- The IP protocol must be UDP (17).
- The UDP destination port must be for TFTP, Domain Name System (DNS), Time, NetBIOS, ND, BOOTP or DHCP packet, or a UDP port specified by the **ip forward-protocol udp** command in global configuration mode.

If the DHCP server resides in a VPN or global space that is different from the interface VPN, then the **vrf** *name* or the **global** option allows you to specify the name of the VRF or global space in which the DHCP server resides.

The **ip helper-addressvrf***name address* option uses the address associated with the VRF name regardless of the VRF of the incoming interface. If the **ip helper-addressvrf***name address* command is configured and later the VRF is deleted from the configuration, then all IP helper addresses associated with that VRF name will be removed from the interface configuration.

If the **ip helper-address** *address* command is already configured on an interface with no VRF name configured, and later the interface is configured with the **ip helper-address vrf** *name address* command, then the previously configured **ip helper-address** *address* command is considered to be global.

Note The **ip helper-address**command does not work on an X.25 interface on a destination router because the router cannot determine if the packet was intended as a physical broadcast.

The **service dhcp** command must be configured on the router to enable IP helper statements to work with DHCP. If the command is not configured, the DHCP packets will not be relayed through the IP helper statements. The **service dhcp** command is configured by default.

Examples

The following example shows how to define an address that acts as a helper address:

```
Router(config)# interface ethernet 1
Router(config-if)# ip helper-address 10.24.43.2
```

The following example shows how to define an address that acts as a helper address and is associated with a VRF named host1:

```
Router(config)# interface ethernet 1/0
Router(config-if)# ip helper-address vrf host1 10.25.44.2
```

The following example shows how to define an address that acts as a helper address and is associated with a VRG named group1:

```
Router(config)# interface ethernet 1/0
Router(config-if)# ip helper-address 10.25.45.2 redundancy group1
```

Related Commands

Command	Description
ip forward-protocol	Specifies which protocols and ports the router forwards when forwarding broadcast packets.
service dhcp	Enables the DHCP server and relay agent features on the router.

ip http authentication

To specify a particular authentication method for HTTP server users, use the **ip http authentication** command in global configuration mode. To disable a configured authentication method, use the **no** form of this command

ip http authentication { **aaa** { **command-authorization** *level list-name* | **exec-authorization** *list-name* | **login-authentication** *list-name* } | **enable** | **local** }

no ip http authentication { **aaa** { **command-authorization** *level list-name* | **exec-authorization** *list-name* | **login-authentication** *list-name* } | **enable** | **local** }

Syntax Description

aaa	Indicates that the authentication method used for the authentication, authorization, and accounting (AAA) login service should be used for authentication. The AAA login authentication method is specified by the **aaa authentication login default** command, unless otherwise specified by the **login-authentication** *listname* keyword and argument.
command-authorization	Sets the authorization method list for commands at the specified privilege level.
level	Indicates a privilege value from 0 through 15. By default, there are the following three command privilege levels on the router: **1.** 0--Includes the **disable** , **enable** , **exit** , **help** , and **logout** commands. **2.** 1--Includes all user-level commands at the device prompt (>). **3.** 15--Includes all enable-level commands at the device prompt (>).
list-name	Sets the name of the method list.
exec-authorization	Sets the method list for EXEC authorization, which applies authorization for starting an EXEC session.
login-authentication	Sets the method list for login authentication, which enables AAA authentication for logins.
enable	Indicates that the "enable" password should be used for authentication. (This is the default method.)
local	ndicates that the login user name, password and privilege level access combination specified in the local system configuration (by the **username** global configuration command) should be used for authentication and authorization.

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

The **ip http authentication** command specifies the authentication method to be used for login when a client connects to the HTTP server. Use of the **aaa** option is recommended. The **enable**, **local**, and **tacacs** methods should be specified using the **aaa authentication login** command.

The “enable” password method is the default HTTP server authentication method. If the enable password is used as the HTTP server login authentication method, the client connects to the HTTP server with a default privilege level of 15.

Examples

The following example shows how to specify that AAA should be used for authentication for HTTP server users. The AAA login method is configured as the “local” username/password authentication method. This example also shows how to specify using the local username database for login authentication and EXEC authorization of HTTP sessions:

```
Device(config)# ip http authentication aaa authentication login LOCALDB local
Device(config)# aaa authorization exec LOCALDB local
Device(config)# ip http authentication aaa login-authentication LOCALDB
Device(config)# ip http authentication aaa exec-authorization LOCALDB
```

ip http auth-retry

To configure the maximum number of authentication retry attempts within a specific time-window, use the **ip http auth-retry** command.

ip http auth-retry *retry_number* **time-window** *time-in-minutes*

Syntax Description

retry_number	Specifies the maximum number of authentication retry attempts.
time-window	Retry time window in minutes.
time-in-minutes	The time window period in minutes during which the maximum number of authentication retries specified can be attempted.

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 maximum number of authentication retry attempts as 5 in a time-window of 2 minutes:

```
Device# ip http auth-retry 5 time-window 2
```

ip http active-session-modules

To selectively enable HTTP applications that will service incoming HTTP requests from remote clients, use the **ip http active-session-modules** command. Use the **no** form of this command to return to the default, for which all HTTP services will be enabled.

ip http active-session-modules { *list-name* | **all** | **none** }

no ip http active-session-modules { *list-name* | **all** | **none** }

Syntax Description

list-name	Enables only those HTTP services configured in the list identified by the **ip http session-module-list** command to serve HTTP requests. All other HTTP or HTTPS applications on the controller will be disabled.
all	Enables all HTTP applications to service incoming HTTP requests from remote clients.
none	Disables all HTTP services.

Command Default

If no arguments or keywords are specified, all HTTP services are enabled.

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

Use the **ip http active-session-modules** command to selectively enable HTTP applications, for servicing incoming HTTP requests from remote clients. With this command, a selected list of applications can be enabled. All the applications can be enabled or none of the applications can be enabled, in other words, all disabled. Use the **ip http session-module-list** command to define a list of HTTP or secure HTTP (HTTPS) application names to be enabled. If an HTTP request is made for a service that is disabled, a 404 error message is displayed in the remote client browser.

Examples

The following example shows how to configure a different set of services to be available for HTTP and HTTPS requests. In this example, all HTTP applications are enabled for providing services to remote clients, but for HTTPS services, only the HTTPS applications defined in list1 (Simple Certificate Enrollment Protocol [SCEP] and HOME_PAGE) are enabled:

```
Device# ip http session-module-list list1 SCEP,HOME_PAGE
ip http active-session-modules all
ip http server
ip http secure-server
ip http secure-active-session-modules list1
```

ip http client secure-ciphersuite

To specify the CipherSuite that should be used for encryption over the secure HTTP connection from the client to a remote server, use the **ip http client secure-ciphersuite** command in global configuration mode. To remove a previously configured CipherSuite specification for the client, use the **no** form of this command.

ip http client secure-ciphersuite [**3des-ede-cbc-sha**] [**rc4-128-sha**] [**rc4-128-md5**] [**des-cbc-sha**]
no ip http client secure-ciphersuite

Syntax Description

3des-ede-cbc-sha	SSL_RSA_WITH_3DES_EDE_CBC_SHA--Rivest, Shamir, and Adleman (RSA) key exchange with 3DES and DES-EDE3-CBC for message encryption and Secure Hash Algorithm (SHA) for message digest.
rc4-128-sha	SSL_RSA_WITH_RC4_128_SHA--RSA key exchange (RSA Public Key Cryptography) with RC4 128-bit encryption for message encryption and SHA for message digest.
rc4-128-md5	SSL_RSA_WITH_RC4_128_MD5--RSA key exchange (RSA Public Key Cryptography) with RC4 128-bit encryption for message encryption and Message Digest 5 (MD5) for message digest.
des-cbc-sha	SSL_RSA_WITH_DES_CBC_SHA--RSA key exchange with DES-CBC for message encryption and SHA for message digest.

Command Default

The client and server negotiate the best CipherSuite that they both support from the list of available CipherSuites.

Command Modes

Global configuration

Command History

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

Usage Guidelines

This command allows you to restrict the list of CipherSuites (encryption algorithms) that the client offers when connecting to a secure HTTP server. For example, you may want to allow only the most secure CipherSuites to be used.

Unless you have a reason to specify the CipherSuites that should be used, or you are unfamiliar with the details of these CipherSuites, you should leave this command unconfigured and let the server and client negotiate the CipherSuite that they both support (this is the default). The **no** form of this command returns the list of available CipherSuites to the default (that is, all CipherSuites supported on your device are available for negotiation).

Examples

The following example shows how to configure the HTTPS client to use only the SSL_RSA_WITH_3DES_EDE_CBC_SHA CipherSuite:

```
Router(config)# ip http client secure-ciphersuite 3des-ede-cbc-sha
```

ip http secure-ciphersuite

To specify the CipherSuites that should be used by the secure HTTP server when negotiating a connection with a remote client, use the **ip http secure-ciphersuite** command in global configuration mode. To return the configuration to the default set of CipherSuites, use the **no** form of this command.

ip http secure-ciphersuite [**3des-ede-cbc-sha**] [**rc4-128-sha**] [**rc4-128-md5**] [**des-cbc-sha**]
no ip http secure-ciphersuite

Syntax Description

3des-ede-cbc-sha	SSL_RSA_WITH_3DES_EDE_CBC_SHA--Rivest, Shamir, and Adleman (RSA) key exchange with 3DES and DES-EDE3-CBC for message encryption and Secure Hash Algorithm (SHA) for message digest.
rc4-128-sha	SSL_RSA_WITH_RC4_128_SHA --RSA key exchange (RSA Public Key Cryptography) with RC4 128-bit encryption for message encryption and SHA for message digest.
rc4-128-md5	SSL_RSA_WITH_RC4_128_MD5 --RSA key exchange (RSA Public Key Cryptography) with RC4 128-bit encryption for message encryption and Message Digest 5 (MD5) for message digest.
des-cbc-sha	SSL_RSA_WITH_DES_CBC_SHA--RSA key exchange with DES-CBC for message encryption and SHA for message digest.

Command Default

The HTTPS server negotiates the best CipherSuite using the list received from the connecting client.

Command Modes

Global configuration

Command History

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

Usage Guidelines

This command is used to restrict the list of CipherSuites (encryption algorithms) that should be used for encryption over the HTTPS connection. For example, you may want to allow only the most secure CipherSuites to be used.

Unless you have a reason to specify the CipherSuites that should be used, or you are unfamiliar with the details of these CipherSuites, you should leave this command unconfigured and let the server and client negotiate the CipherSuite that they both support (this is the default).

The supported CipherSuites vary by Cisco IOS software image. For example, “IP Sec56” (“k8”) images support only the SSL_RSA_WITH_DES_CBC_SHA CipherSuite in Cisco IOS Release 12.2(15)T.

In terms of router processing load (speed), the following list ranks the CipherSuites from fastest to slowest (slightly more processing time is required for the more secure and more complex CipherSuites):

1. SSL_RSA_WITH_DES_CBC_SHA
2. SSL_RSA_WITH_RC4_128_MD5
3. SSL_RSA_WITH_RC4_128_SHA

4. SSL_RSA_WITH_3DES_EDE_CBC_SHA

Additional information about these CipherSuites can be found online from sources that document the Secure Sockets Layer (SSL) 3.0 protocol.

Examples

The following exampleshows how to restrictsthe CipherSuites offered to a connecting secure web client:

```
Router(config)# ip http secure-ciphersuite rc4-128-sha rc4-128-md5
```

ip http secure-server

To enable a secure HTTP (HTTPS) server, enter the **ip http secure-server** command in global configuration mode. To disable the HTTPS server, use the **no** form of this command..

ip http secure-server
no ip http secure-server

Syntax Description

This command has no arguments or keywords.

Command Default

The HTTPS server is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1 Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

The HTTPS server uses the Secure Sockets Layer (SSL) version 3.0 protocol.

⚠

Caution When enabling an HTTPS server, you should always disable the standard HTTP server to prevent unsecured connections to the same services. Disable the standard HTTP server using the **no ip http server** command in global configuration mode (this step is precautionary; typically, the HTTP server is disabled by default).

If a certificate authority (CA) is used for certification, you should declare the CA trustpoint on the routing device before enabling the HTTPS server.

To close HTTP/TCP port 8090, you must disable both the HTTP and HTTPS servers. Enter the **no http server** and the **no http secure-server** commands, respectively.

Examples

In the following example the HTTPS server is enabled, and the (previously configured) CA trustpoint CA-trust-local is specified:

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#ip http secure-server
Device(config)#ip http secure-trustpoint CA-trust-local
Device(config)#end

Device#show ip http server secure status
HTTP secure server status: Enabled
HTTP secure server port: 443
HTTP secure server ciphersuite: 3des-ede-cbc-sha des-cbc-sha rc4-128-md5 rc4-12a
HTTP secure server client authentication: Disabled
HTTP secure server trustpoint: CA-trust-local
```

Related Commands

Command	Description
ip http secure-trustpoint	Specifies the CA trustpoint that should be used for obtaining signed certificates for the HTTPS server.
ip http server	Enables the HTTP server on an IP or IPv6 system, including the Cisco web browser user interface.
show ip http server secure status	Displays the configuration status of the HTTPS server.

ip http server

To enable the HTTP server on your IP or IPv6 system, including the Cisco web browser user interface, enter the **ip http server** command in global configuration mode. To disable the HTTP server, use the **no** form of this command..

ip http server
no ip http server

Syntax Description

This command has no arguments or keywords.

Command Default

The HTTP server uses the standard port 80 by default.

HTTP/TCP port 8090 is open by default.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

The command enables both IPv4 and IPv6 access to the HTTP server. However, an access list configured with the **ip http access-class** command is applied only to IPv4 traffic. IPv6 traffic filtering is not supported.

Caution The standard HTTP server and the secure HTTP (HTTPS) server can run on a system at the same time. If you enable the HTTPS server using the **ip http secure-server** command, disable the standard HTTP server using the **no ip http server** command to ensure that secure data cannot be accessed through the standard HTTP connection.

To close HTTP/TCP port 8090, you must disable both the HTTP and HTTPS servers. Enter the **no http server** and the **no http secure-server** commands, respectively.

Examples

The following example shows how to enable the HTTP server on both IPv4 and IPv6 systems.

After enabling the HTTP server, you can set the base path by specifying the location of the HTML files to be served. HTML files used by the HTTP web server typically reside in system flash memory. Remote URLs can be specified using this command, but use of remote path names (for example, where HTML files are located on a remote TFTP server) is not recommended.

```
Device(config)#ip http server
Device(config)#ip http path flash:
```

Related Commands

Command	Description
ip http access-class	Specifies the access list that should be used to restrict access to the HTTP server.

Command	Description
ip http path	Specifies the base path used to locate files for use by the HTTP server.
ip http secure-server	Enables the HTTPS server.

ip http session-module-list

To define a list of HTTP or secure HTTP application names, use the **ip http session-module-list** command in global configuration mode. To remove the defined list, use the **no** form of this command.

ip http session-module-list *listname prefix1* [*prefix2,...prefixn*]

no ip http session-module-list *listname prefix1* [*prefix2,...prefixn*]

Syntax Description

listname	Name of the list.
prefix 1	Associated HTTP or HTTPS application names. Prefix strings represent the names of applications, for example, SCEP, WEB_EXEC or HOME_PAGE.
prefix2,...prefixn	(Optional) Additional associated HTTP or HTTPS application names. Each application is separated by a comma.

Command Default

No list of HTTP or HTTPS application names is defined.

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

Use this command to define a list of HTTP or HTTPS application names. The defined list can then be used by the **ip http active-session-modules** or **ip http secure-active-session-modules** commands to selectively enable HTTP or HTTPS applications, respectively, for servicing incoming HTTP and HTTPS requests from remote clients.

When defining a list of HTTP or HTTPS application names, use the following guidelines:

- A maximum of four lists can be defined on a controller. Attempts to define more than four lists will fail and an error message will be displayed stating the limit restrictions.
- An existing list can be removed using the **no ip http session-module-list** command.
- You cannot reconfigure an existing list. Instead of reconfiguring an existing list, remove the existing list and create a new list with the same name.
- There is no limit to how many application names can be in the list. However, the maximum number of sessions that can be registered with the Cisco IOS HTTP or HTTPS server is 32.

Examples

The following example shows how to configure a different set of services to be available for HTTP and HTTPS requests. In this example, all HTTP applications are enabled for providing services to remote clients, but for HTTPS services, only the HTTPS applications defined in list1 (Simple Certificate Enrollment Protocol [SCEP] and HOME_PAGE) are enabled:

```
Device# ip http session-module-list list1 SCEP,HOME_PAGE
Device# ip http active-session-modules all
```

```
Device# ip http server
Device# ip http secure-server
Device# ip http secure-active-session-modules list1
```

ip ssh

To configure Secure Shell (SSH) control parameters on your router, use the **ip ssh** command in global configuration mode. To restore the default value, use the **no** form of this command.

ip ssh [**timeout** *seconds* | **authentication-retries** *integer*]
no ip ssh [**timeout** *seconds* | **authentication-retries** *integer*]

Syntax Description

timeout	(Optional) The time interval that the router waits for the SSH client to respond. This setting applies to the SSH negotiation phase. Once the EXEC session starts, the standard timeouts configured for the vty apply. By default, there are 5 vtys defined (0-4), therefore 5 terminal sessions are possible. After the SSH executes a shell, the vty timeout starts. The vty timeout defaults to 10 minutes.
seconds	(Optional) The number of seconds until timeout disconnects, with a maximum of 120 seconds. The default is 120 seconds.
authentication- retries	(Optional) The number of attempts after which the interface is reset.
integer	(Optional) The number of retries, with a maximum of 5 authentication retries. The default is 3.

Command Default

SSH control parameters are set to default router values.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1) T.
12.2(17a)SX	This command was integrated into Cisco IOS Release 12.2(17a)SX.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

Before you configure SSH on your router, you must enable the SSH server using the **crypto key generate rsa**command.

Examples

The following examples configure SSH control parameters on your router:

```
ip ssh timeout 120
ip ssh authentication-retries 3
```

ip ssh version

To specify the version of Secure Shell (SSH) to be run on a router, use the **ip ssh version**command in global configuration mode. To disable the version of SSH that was configured and to return to compatibility mode, use the **no** form of this command.

ip ssh version [**1** | **2**]
no ip ssh version [**1** | **2**]

Syntax Description

1	(Optional) Router runs only SSH Version 1.
2	(Optional) Router runs only SSH Version 2.

Command Default

If this command is not configured, SSH operates in compatibility mode, that is, Version 1 and Version 2 are both supported.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.3(2)XE	This command was integrated into Cisco IOS Release 12.3(2)XE.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(7)JA	This command was integrated into Cisco IOS Release 12.3(7)JA.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
15.2(2)SA2	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.

Usage Guidelines

You can use this command with the **2** keyword to ensure that your router will not inadvertently establish a weaker SSH Version 1 connection.

Examples

The following example shows that only SSH Version 1 support is configured:

```
Router (config)# ip ssh version 1
```

The following example shows that only SSH Version 2 is configured:

```
Router (config)# ip ssh version 2
```

The following example shows that SSH Versions 1 and 2 are configured:

```
Router (config)# no ip ssh version
```

Related Commands

Command	Description
debug ip ssh	Displays debug messages for SSH.
disconnect ssh	Terminates a SSH connection on your router.
ip ssh	Configures SSH control parameters on your router.
ip ssh rsa keypair-name	Specifies which RSA key pair to use for a SSH connection.
show ip ssh	Displays the SSH connections of your router.

ip tftp blocksize

To specify TFTP client blocksize, use the **ip tftp blocksize** command.

ip tftp blocksize *blocksize-value*

Syntax Description

blocksize-value	Blocksize value. Valid range is from 512-8192 Kbps.

Command Default

TFTP client blocksize is not configured.

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

Use this command to change the default blocksize to decrease the image download time.

Example

The following example shows how to specify TFTP client blocksize:

```
Device(config)# ip tftp blocksize 512
```

ip verify source

To enable IP source guard on an interface, use the **ip verify source** command in interface configuration mode. To disable IP source guard, use the **no** form of this command.

ip verify source
no ip verify source

Command Default

IP source guard is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1 Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

To enable IP source guard with source IP address filtering, use the **ip verify source** interface configuration command.

Examples

This example shows how to enable IP source guard with source IP address filtering on an interface:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip verify source
```

You can verify your settings by entering the **show ip verify source** privileged EXEC command.

ipv4-address-type

To configure the 802.11u IPv4 address type, use the **ipv4-address-type** command. To remove the address type, use the **no** form of the command.

ipv4-address-type
{**double-nated-private** | **not-available** | **not-known** | **port-restricted** | **port-restricted-double-nated** | **port-restricted-single-nated** | **public** | **single-nated-private**}

Syntax Description

double-nated-private	Sets IPv4 address as double network address translation (NAT) private.
not-available	Sets IPv4 address type as not available.
not-known	Sets IPv4 address type availability as not known.
port-restricted	Sets IPv4 address type as port-restricted.
port-restricted-double-nated	Sets IPv4 address type as port-restricted and double NATed.
port-restricted-single-nated	Sets IPv4 address type as port-restricted and single NATed.
public	Sets IPv4 address type as public.
single-nated-private	Sets IPv4 address as single NATed private.

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 a 802.11u IPv4 address type:

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# ipv4-address-type public
```

ipv4 dhcp

To configure the DHCP parameters for a WLAN, use the **ipv4 dhcp** command.

ipv4 dhcp {**opt82** | {**ascii** | **rid** | **format** | {**ap_ethmac** | **ap_location** | **apmac** | **apname** | **policy_tag** | **ssid** | **vlan_id** }} | **required** | **server** *dhcp-ip-addr*}

Syntax Description

opt82	Sets DHCP option 82 for wireless clients on this WLAN
required	Specifies whether DHCP address assignment is required
server	Configures the WLAN's IPv4 DHCP Server
ascii	Supports ASCII for DHCP option 82
rid	Supports adding Cisco 2 byte RID for DHCP option 82
format	Sets RemoteID format
ap_ethmac	Enables DHCP AP Ethernet MAC address
ap_location	Enables AP location
apmac	Enables AP MAC address
apname	Enables AP name
site_tag (Policy tag)	Enables Site tag
ssid	Enables SSID
vlan_id	Enables VLAN ID
dhcp-ip-addr	Enter the override DHCP server's IP Address.

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 DHCP address assignment as a requirement:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy demo-profile-name
Device(config-wireless-policy)# ipv4 dhcp required
```

ipv4 flow monitor

To configure the IPv4 traffic ingress flow monitor for a WLAN profile policy, use the **ipv4 flow monitor input** command.

ipv4 flow monitor *monitor-name* **input**

Syntax Description

monitor-name	Flow monitor name.
input	Enables flow monitor on ingress traffic.

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 the IPv4 traffic ingress flow monitor for a WLAN profile policy:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy policy-profile-name
Device(config-wireless-policy)# ipv4 flow monitor flow-monitor-name input
```

ipv6 access-list

To define an IPv6 access list and to place the device in IPv6 access list configuration mode, use the **ipv6 access-list** command in global configuration mode. To remove the access list, use the **no** form of this command.

ipv6 access-list *access-list-name* | **match-local-traffic** | **log-update threshold** *threshold-in-msgs* | **role-based** *list-name*
noipv6 access-list *access-list-name* | **client** *permit-control-packets* | **log-update** *threshold* | **role-based** *list-name*

Syntax Description

ipv6 *access-list-name*	Creates a named IPv6 ACL (up to 64 characters in length) and enters IPv6 ACL configuration mode. *access-list-name* - Name of the IPv6 access list. Names cannot contain a space or quotation mark, or begin with a numeric.
match-local-traffic	Enables matching for locally-generated traffic.
log-update threshold *threshold-in-msgs*	Determines how syslog messages are generated after the initial packet match. *threshold-in-msgs*- Number of packets generated.
role-based *list-name*	Creates a role-based IPv6 ACL.

Command Default

No IPv6 access list is defined.

Command Modes

Global configuration

Command History

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

Usage Guidelines

IPv6 ACLs are defined by using the **ipv6 access-list**command in global configuration mode and their permit and deny conditions are set by using the **deny** and **permit**commands in IPv6 access list configuration mode. Configuring the **ipv6 access-list**command places the device in IPv6 access list configuration mode--the device prompt changes to Device(config-ipv6-acl)#. From IPv6 access list configuration mode, permit and deny conditions can be set for the defined IPv6 ACL.

Note IPv6 ACLs are defined by a unique name (IPv6 does not support numbered ACLs). An IPv4 ACL and an IPv6 ACL cannot share the same name.

IPv6 is automatically configured as the protocol type in **permit any any** and **deny any any** statements that are translated from global configuration mode to IPv6 access list configuration mode.

Every IPv6 ACL has implicit **permit icmp any any nd-na**, **permit icmp any any nd-ns**, and **deny ipv6 any any** statements as its last match conditions. (The former two match conditions allow for ICMPv6 neighbor

discovery.) An IPv6 ACL must contain at least one entry for the implicit **deny ipv6 any any** statement to take effect. The IPv6 neighbor discovery process makes use of the IPv6 network layer service; therefore, by default, IPv6 ACLs implicitly allow IPv6 neighbor discovery packets to be sent and received on an interface. In IPv4, the Address Resolution Protocol (ARP), which is equivalent to the IPv6 neighbor discovery process, makes use of a separate data link layer protocol; therefore, by default, IPv4 ACLs implicitly allow ARP packets to be sent and received on an interface.

Use the **ipv6 traffic-filter** interface configuration command with the *access-list-name* argument to apply an IPv6 ACL to an IPv6 interface. Use the **ipv6 access-class** line configuration command with the *access-list-name* argument to apply an IPv6 ACL to incoming and outgoing IPv6 virtual terminal connections to and from the device.

An IPv6 ACL applied to an interface with the **ipv6 traffic-filter** command filters traffic that is forwarded, not originated, by the device.

Examples

The example configures the IPv6 ACL list named list1 and places the device in IPv6 access list configuration mode.

```
Device(config)# ipv6 access-list list1
Device(config-ipv6-acl)#
```

The following example configures the IPv6 ACL named list2 and applies the ACL to outbound traffic on Ethernet interface 0. Specifically, the first ACL entry keeps all packets from the network FEC0:0:0:2::/64 (packets that have the site-local prefix FEC0:0:0:2 as the first 64 bits of their source IPv6 address) from exiting out of Ethernet interface 0. The second entry in the ACL permits all other traffic to exit out of Ethernet interface 0. The second entry is necessary because an implicit deny all condition is at the end of each IPv6 ACL.

```
Device(config)# ipv6 access-list list2 deny FEC0:0:0:2::/64 any
Device(config)# ipv6 access-list list2 permit any any
Device(config)# interface ethernet 0
Device(config-if)# ipv6 traffic-filter list2 out
```

ipv6-address-type

To configure the 802.11u IPv6 address type, use the **ipv6-address-type** command. To remove the address type, use the **no** form of the command.

ipv6-address-type {**available** | **not-available** | **not-known**}

Syntax Description

available	Sets IPv6 address type as available.
not-available	Sets IPv6 address type as not available.
not-known	Sets IPv6 address type availability as not known.

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 IPv6 address type:

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# ipv4-address-type available
```

ipv6 address

To configure an IPv6 address based on an IPv6 general prefix and enable IPv6 processing on an interface, use the **ipv6 address**command in interface configuration mode. To remove the address from the interface, use the **no** form of this command.

ipv6 address {*ipv6-prefix/prefix-length* | *prefix-name sub-bits/prefix-length*}
no ipv6 address {*ipv6-address/prefix-length* | *prefix-name sub-bits/prefix-length*}

Syntax Description

ipv6-address	The IPv6 address to be used.
/ *prefix-length*	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
prefix-name	A general prefix, which specifies the leading bits of the network to be configured on the interface.
sub-bits	The subprefix bits and host bits of the address to be concatenated with the prefixes provided by the general prefix specified with the *prefix-name* argument. The *sub-bits*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

No IPv6 addresses are defined for any interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
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.
Cisco IOS XE Release 2.1	This command was integrated into Cisco ASR 1000 Series devices.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.2(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services devices.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **ipv6 address** command allows multiple IPv6 addresses to be configured on an interface in various different ways, with varying options. The most common way is to specify the IPv6 address with the prefix length.

Addresses may also be defined using the general prefix mechanism, which separates the aggregated IPv6 prefix bits from the subprefix and host bits. In this case, the leading bits of the address are defined in a general prefix, which is globally configured or learned (for example, through use of Dynamic Host Configuration Protocol-Prefix Delegation (DHCP-PD)), and then applied using the *prefix-name* argument. The subprefix bits and host bits are defined using the *sub-bits* argument.

Using the **no ipv6 address autoconfig** command without arguments removes all IPv6 addresses from an interface.

IPv6 link-local addresses must be configured and IPv6 processing must be enabled on an interface by using the **ipv6 address link-local** command.

Examples

The following example shows how to enable IPv6 processing on the interface and configure an address based on the general prefix called my-prefix and the directly specified bits:

```
Device(config-if) ipv6 address my-prefix 0:0:0:7272::72/64
```

Assuming the general prefix named my-prefix has the value of 2001:DB8:2222::/48, then the interface would be configured with the global address 2001:DB8:2222:7272::72/64.

Related Commands

Command	Description
ipv6 address anycast	Configures an IPv6 anycast address and enables IPv6 processing on an interface.
ipv6 address eui-64	Configures an IPv6 address and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address.
ipv6 address link-local	Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface.
ipv6 unnumbered	Enables IPv6 processing on an interface without assigning an explicit IPv6 address to the interface.
no ipv6 address autoconfig	Removes all IPv6 addresses from an interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 dhcp pool

To configure a Dynamic Host Configuration Protocol (DHCP) for IPv6 server configuration information pool and enter DHCP for IPv6 pool configuration mode, use the **ipv6 dhcp pool** command in global configuration mode. To delete a DHCP for IPv6 pool, use the **no** form of this command.

ipv6 dhcp pool *poolname*
no ipv6 dhcp pool *poolname*

Syntax Description

poolname	User-defined name for the local prefix pool. The pool name can be a symbolic string (such as "Engineering") or an integer (such as 0).

Command Default

DHCP for IPv6 pools are not configured.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.
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

Use the **ipv6 dhcp pool**command to create a DHCP for IPv6 server configuration information pool. When the **ipv6 dhcp pool** command is enabled, the configuration mode changes to DHCP for IPv6 pool configuration mode. In this mode, the administrator can configure pool parameters, such as prefixes to be delegated and Domain Name System (DNS) servers, using the following commands:

- **address prefix** *IPv6-prefix* [**lifetime** {*valid-lifetime preferred-lifetime* | **infinite**}]sets an address prefix for address assignment. This address must be in hexadecimal, using 16-bit values between colons.
- **link-address** *IPv6-prefix* sets a link-address IPv6 prefix. When an address on the incoming interface or a link-address in the packet matches the specified IPv6-prefix, the server uses the configuration information pool. This address must be in hexadecimal, using 16-bit values between colons.
- **vendor-specific** *vendor-id* enables DHCPv6 vendor-specific configuration mode. Specify a vendor identification number. This number is the vendor IANA Private Enterprise Number. The range is 1 to 4294967295. The following configuration command is available:
  - **suboption** *number* sets vendor-specific suboption number. The range is 1 to 65535. You can enter an IPv6 address, ASCII text, or a hex string as defined by the suboption parameters.

Note The **hex** value used under the **suboption** keyword allows users to enter only hex digits (0-f). Entering an invalid **hex** value does not delete the previous configuration.

Once the DHCP for IPv6 configuration information pool has been created, use the **ipv6 dhcp server** command to associate the pool with a server on an interface. If you do not configure an information pool, you need to use the **ipv6 dhcp server interface** configuration command to enable the DHCPv6 server function on an interface.

When you associate a DHCPv6 pool with an interface, only that pool services requests on the associated interface. The pool also services other interfaces. If you do not associate a DHCPv6 pool with an interface, it can service requests on any interface.

Not using any IPv6 address prefix means that the pool returns only configured options.

The **link-address** command allows matching a link-address without necessarily allocating an address. You can match the pool from multiple relays by using multiple link-address configuration commands inside a pool.

Since a longest match is performed on either the address pool information or the link information, you can configure one pool to allocate addresses and another pool on a subprefix that returns only configured options.

Examples

The following example specifies a DHCP for IPv6 configuration information pool named cisco1 and places the router in DHCP for IPv6 pool configuration mode:

```
Router(config)# ipv6 dhcp pool cisco1
Router(config-dhcpv6)#
```

The following example shows how to configure an IPv6 address prefix for the IPv6 configuration pool cisco1:

```
Router(config-dhcpv6)# address prefix 2001:1000::0/64
Router(config-dhcpv6)# end
```

The following example shows how to configure a pool named engineering with three link-address prefixes and an IPv6 address prefix:

```
Router# configure terminal
Router(config)# ipv6 dhcp pool engineering
Router(config-dhcpv6)# link-address 2001:1001::0/64
Router(config-dhcpv6)# link-address 2001:1002::0/64
Router(config-dhcpv6)# link-address 2001:2000::0/48
Router(config-dhcpv6)# address prefix 2001:1003::0/64
Router(config-dhcpv6)# end
```

The following example shows how to configure a pool named 350 with vendor-specific options:

```
Router# configure terminal
Router(config)# ipv6 dhcp pool 350
Router(config-dhcpv6)# vendor-specific 9
Router(config-dhcpv6-vs)# suboption 1 address 1000:235D::1
Router(config-dhcpv6-vs)# suboption 2 ascii "IP-Phone"
Router(config-dhcpv6-vs)# end
```

Related Commands

Command	Description
ipv6 dhcp server	Enables DHCP for IPv6 service on an interface.
show ipv6 dhcp pool	Displays DHCP for IPv6 configuration pool information.

ipv6 enable

To enable IPv6 processing on an interface that has not been configured with an explicit IPv6 address, use the **ipv6 enable**command in interface configuration mode. To disable IPv6 processing on an interface that has not been configured with an explicit IPv6 address, use the **no** form of this command.

ipv6 enable
no ipv6 enable

Syntax Description

This command has no arguments or keywords.

Command Default

IPv6 is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
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.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.2(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services devices.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.
15.2(2)SA2	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.

Usage Guidelines

The **ipv6 enable**command automatically configures an IPv6 link-local unicast address on the interface while also enabling the interface for IPv6 processing. The no **ipv6 enable**command does not disable IPv6 processing on an interface that is configured with an explicit IPv6 address.

Examples

The following example enables IPv6 processing on Ethernet interface 0/0:

```
Device(config)# interface ethernet 0/0
Device(config-if)# ipv6 enable
```

Related Commands

Command	Description
ipv6 address link-local	Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface.
ipv6 address eui-64	Configures an IPv6 address and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address.
ipv6 unnumbered	Enables IPv6 processing on an interface without assigning an explicit IPv6 address to the interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 mld snooping

To enable Multicast Listener Discovery version 2 (MLDv2) protocol snooping globally, use the **ipv6 mld snooping** command in global configuration mode. To disable the MLDv2 snooping globally, use the **no** form of this command.

ipv6 mld snooping
no ipv6 mld snooping

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

MLDv2 snooping is supported on the Supervisor Engine 720 with all versions of the Policy Feature Card 3 (PFC3).

To use MLDv2 snooping, configure a Layer 3 interface in the subnet for IPv6 multicast routing or enable the MLDv2 snooping querier in the subnet.

Examples

This example shows how to enable MLDv2 snooping globally:

```
Router(config)# ipv6 mld snooping
```

Related Commands

Command	Description
show ipv6 mld snooping	Displays MLDv2 snooping information.

ipv6 nd managed-config-flag

To set the managed address configuration flag in IPv6 router advertisements, use the **ipv6 nd managed-config-flag** command in an appropriate configuration mode. To clear the flag from IPv6 router advertisements, use the **no** form of this command.

ipv6 nd managed-config-flag
no ipv6 nd managed-config-flag

Syntax Description

This command has no keywords or arguments.

Command Default

The managed address configuration flag is not set in IPv6 router advertisements.

Command Modes

Interface 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 managed address configuration flag in IPv6 router advertisements indicates to attached hosts whether they should use stateful autoconfiguration to obtain addresses. If the flag is set, the attached hosts should use stateful autoconfiguration to obtain addresses. If the flag is not set, the attached hosts should not use stateful autoconfiguration to obtain addresses.

Hosts may use stateful and stateless address autoconfiguration simultaneously.

Examples

This example shows how to configure the managed address configuration flag in IPv6 router advertisements:

```
Device(config)# interface
Device(config-if)# ipv6 nd managed-config-flag
```

ipv6 nd other-config-flag

To set the other stateful configuration flag in IPv6 router advertisements, use the **ipv6 nd other-config-flag** command in an appropriate configuration mode. To clear the flag from IPv6 router advertisements, use the **no** form of this command.

ipv6 nd other-config-flag

Syntax Description

This command has no keywords or arguments.

Command Default

The other stateful configuration flag is not set in IPv6 router advertisements.

Command Modes

Interface configuration

Dynamic template 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

The setting of the other stateful configuration flag in IPv6 router advertisements indicates to attached hosts how they can obtain autoconfiguration information other than addresses. If the flag is set, the attached hosts should use stateful autoconfiguration to obtain the other (nonaddress) information.

Note If the managed address configuration flag is set using the **ipv6 nd managed-config-flag** command, then an attached host can use stateful autoconfiguration to obtain the other (nonaddress) information regardless of the setting of the other stateful configuration flag.

Examples

This example (not applicable for BNG) configures the “other stateful configuration” flag in IPv6 router advertisements:

```
Device(config)# interface
Device(config-if)# ipv6 nd other-config-flag
```

ipv6 nd ra throttler attach-policy

To configure a IPv6 policy for feature RA throttler, use the **ipv6 nd ra-throttler attach-policy** command.

ipv6 nd ra-throttler attach-policy *policy-name*

Syntax Description

ipv6	IPv6 root chain.
ra-throttler	Configure RA throttler on the VLAN.
attach-policy	Apply a policy for feature RA throttler.
policy-name	Policy name for feature RA throttler

Command Default

None

Command Modes

config-vlan

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 configure a IPv6 policy for feature RA throttler:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# vlan configuration vlan-id
Device(config-vlan-config)# ipv6 nd ra-throttler attach-policy
```

ipv6 nd raguard policy

To define the router advertisement (RA) guard policy name and enter RA guard policy configuration mode, use the **ipv6 nd raguard policy** command in global configuration mode.

ipv6 nd raguardpolicy *policy-name*

Syntax Description

policy-name	IPv6 RA guard policy name.

Command Default

An RA guard policy is not configured.

Command Modes

Global configuration (config)#

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

Use the **ipv6 nd raguard policy** command to configure RA guard globally on a router. Once the device is in ND inspection policy configuration mode, you can use any of the following commands:

- **device-role**
- **drop-unsecure**
- **limit address-count**
- **sec-level minimum**
- **trusted-port**
- **validate source-mac**

After IPv6 RA guard is configured globally, you can use the **ipv6 nd raguard attach-policy** command to enable IPv6 RA guard on a specific interface.

Examples

The following example shows how to define the RA guard policy name as policy1 and place the device in policy configuration mode:

```
Device(config)# ipv6 nd raguard policy policy1
Device(config-ra-guard)#
```

Related Commands

Table 1:

Command	Description
device-role	Specifies the role of the device attached to the port.
drop-unsecure	Drops messages with no or invalid options or an invalid signature.
ipv6 nd raguard attach-policy	Applies the IPv6 RA guard feature on a specified interface.
limit address-count	Limits the number of IPv6 addresses allowed to be used on the port.
sec-level minimum	Specifies the minimum security level parameter value when CGA options are used.
trusted-port	Configures a port to become a trusted port.
validate source-mac	Checks the source MAC address against the link layer address.

ipv6 traffic-filter

This command enables IPv6 traffic filter.

To enable the filtering of IPv6 traffic on an interface, use the **ipv6 traffic-filter** command. To disable the filtering of IPv6 traffic on an interface, use the **no** form of the command.

Use the **ipv6 traffic-filter** interface configuration command on the switch stack or on a standalone switch to filter IPv6 traffic on an interface. The type and direction of traffic that you can filter depends on the feature set running on the switch stack. Use the **no** form of this command to disable the filtering of IPv6 traffic on an interface.

ipv6 traffic-filter [**web**] *acl-name*
no ipv6 traffic-filter [**web**]

Syntax Description

web	(Optional) Specifies an IPv6 access name for the WLAN Web ACL.
acl-name	Specifies an IPv6 access name.

Command Default

Filtering of IPv6 traffic on an interface is not configured.

Command Modes

wlan

Command History

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

Usage Guidelines

To configure the dual IPv4 and IPv6 template, enter the **sdm prefer dual-ipv4-and-ipv6 {default | vlan}** global configuration command and reload the switch.

You can use the **ipv6 traffic-filter** command on physical interfaces (Layer 2 or Layer 3 ports), Layer 3 port channels, or switch virtual interfaces (SVIs).

You can apply an ACL to outbound or inbound traffic on Layer 3 interfaces (port ACLs), or to inbound traffic on Layer 2 interfaces (router ACLs).

If **any** port ACL (IPv4, IPv6, or MAC) is applied to an interface, that port ACL is used to filter packets, and any router ACLs attached to the SVI of the port VLAN are ignored.

This example shows how to filter IPv6 traffic on an interface:

```
Device(config-wlan)# ipv6 traffic-filter TestDocTrafficFilter
```

key chain

To create or modify a keychain, use the **key chain** command. To disable this feature, use the **no** form of this command.

key chain*key-chain name* { **macsec** | **tcp** }
no key chain*key-chain name* { **macsec** | **tcp** }

Syntax Description

key-chain name	Specifies the name of the key chain.
macsec	Specifies a MacSEC key chain.
tcp	Specifies the tcp key chain.

Command Default

No default.

Command Modes

Global configuration mode.

Examples

The following example shows how to specify a key chain to identify authentication on a key-chain:

```
Device(config)# key chain key-chain-name macsec
```

Related Commands

Command	Description
key config-key	Sets a private configuration key for general use.
show key chain	Displays authentication key information.

key config-key

To set a private configuration key for private use, use the **key config-key** command. To disable this feature, use the **no** form of this command.

key config-key { **1 LINE** | **newpass** *config-key* | **password-encrypt LINE** }
no key config-key { **1 LINE** | **newpass** *config-key* | **password-encrypt LINE** }

Syntax Description

1	Sets a private configuration key for private use.
newpass	Specifies a new password without space or tabs.
config-key	Specifies the config key, with a minimum of 8 characters, and not beginning with the IOS special characters - !, #, and ;.
password-encrypt	Sets a private configuration key for password encryption.

Command Default

None

Command Modes

Global configuration mode.

Examples

The following example shows how to specify a config-key:

```
Device(config)# key config-key password-encrypt config-key
```

key config-key password-encrypt

To set a private configuration key for password encryption, use the **key config-key password-encrypt** command. To disable this feature, use the **no** form of this command.

key config-key password-encrypt <*config-key*>

Syntax Description

config-key	Enter a value with minimum 8 characters. **Note** The value must not begin with the following special characters: !, #, and ;

Command Default

None

Command Modes

Global configuration mode

Command History

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

Examples

The following example shows how to set a username and password for AP management:

```
Device# enable
Device# configure terminal
Device(config)# key config-key password-encryption 12345678
Device(config-ap-profile)# password encryption aes
Device(config-ap-profile)# end
```

license air level

To configure AIR licenses on a wireless controller, enter the **license air level** command in global configuration mode. To revert to the default setting, use the **no** form of this command.

license air level { **air-network-advantage** [**addon air-dna-advantage**] | **air-network-essentials** [**addon air-dna-essentials**] }

no license air level

Syntax Description

air-network-advantage	Configures the AIR Network Advantage license level.
addon air-dna-advantage	(Optional) Configures the add-on AIR DNA Advantage license level. This add-on option is available with the AIR Network Advantage license.
air-network-essentials	Configures the AIR Network Essentials license level.
addon air-dna-essentials	(Optional) Configures the add-on AIR DNA Essentials license level. This add-on option is available with the AIR Network Essential license.

Command Default

For all Cisco Catalyst 9800 Wireless controllers the default license is AIR DNA Advantage.

For EWC-APs:

- Prior to Cisco IOS XE Bengaluru 17.4.1, the default license is AIR DNA Essentials.
- Starting with Cisco IOS XE Bengaluru 17.4.1, the default license is AIR Network Essentials

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2a	This command continues to be available and applicable with the introduction of Smart Licensing Using Policy.
Cisco IOS XE Bengaluru 17.4.1	Only for EWC-APs, the default license was changed from AIR DNA Essentials to AIR Network Essentials.

Usage Guidelines

In the Smart Licensing Using Policy environment, you can use the **license air level** command to change the license level being used on the product instance, or to additionally configure an add-on license on the product instance. The change is effective after a reload.

The licenses that can be configured are:

- AIR Network Essential
- AIR Network Advantage
- AIR DNA Essential

- AIR DNA Advantage

You can configure AIR DNA Essential or AIR DNA Advantage license level and on term expiry, you can move to the Network Advantage or Network Essentials license level, if you do not want to renew the DNA license.

Every connecting AP requires a Cisco DNA Center License to leverage the unique value properties of the controller.

Examples

The following example show how to configure the AIR DNA Essential license level:

```
Device# configure terminal
Device(config)# license air level network-essentials addon air-dna-essentials
```

The following example shows how the AIR DNA Advantage license level is configured to begin with and then changed to AIR DNA Essentials:

Current configuration as AIR DNA Advantage:

```
Device# show version
Cisco IOS XE Software, Version 17.03.02
Cisco IOS Software [Amsterdam], C9800-CL Software (C9800-CL-K9_IOSXE), Version 17.3.2,
RELEASE SOFTWARE
<output truncated>
AIR License Level: AIR DNA Advantage
Next reload AIR license Level: AIR DNA Advantage

Smart Licensing Status: Registration Not Applicable/Not Applicable
<output truncated>
```

Configuration of AIR DNA Essentials :

```
Device# configure terminal
Device(config)# license air level air-network-essentials addon air-dna-essentials

Device# exit
Device# show version
Cisco IOS XE Software, Version 17.03.02
Cisco IOS Software [Amsterdam], C9800-CL Software (C9800-CL-K9_IOSXE), Version 17.3.2,
RELEASE SOFTWARE
<output truncated>
AIR License Level: AIR DNA Advantage
Next reload AIR license Level: AIR DNA Essentials
Smart Licensing Status: Registration Not Applicable/Not Applicable
<output truncated>

Device# write memory
Device# reload
```

After reload:

```
Device# show version
Cisco IOS XE Software, Version 17.03.02
Cisco IOS Software [Amsterdam], C9800-CL Software (C9800-CL-K9_IOSXE), Version 17.3.2,
RELEASE SOFTWARE
<output truncated>
AIR License Level: AIR DNA Essentials
Next reload AIR license Level: AIR DNA Essentials

Smart Licensing Status: Registration Not Applicable/Not Applicable
<output truncated>
```

license smart (global config)

To configure licensing-related settings such as the mode of transport and the URL that the product instance uses to communicate with Cisco Smart Software Manager (CSSM), or Cisco Smart Licensing Utility (CSLU), or Smart Software Manager On-Prem (SSM On-Prem), to configure the usage reporting interval, to configure the information that must be exluded or included in a license usage report (RUM report), enter the **license smart** command in global configuration mode. Use the **no** form of the command to revert to default values.

license smart { **custom_id** *ID* | **enable** | **privacy** { **all** | **hostname** | **version** } | **proxy** { **address** *address_hostname* | **port** *port* } | **reservation** | **server-identity-check** | **transport** { **automatic** | **callhome** | **cslu** | **off** | **smart** } | **url** { *url* | **cslu** *cslu_or_on-prem_url* | **default** | **smart** *smart_url* | **utility** *secondary_url* } | **usage** { **customer-tags** { **tag1** | **tag2** | **tag3** | **tag4** } *tag_value* | **interval** *interval_in_days* } | **utility** [**customer_info** { **city** *city* | **country** *country* | **postalcode** *postalcode* | **state** *state* | **street** *street* }] }

no license smart { **custom_id** | **enable** | **privacy** { **all** | **hostname** | **version** } | **proxy** { **address** *address_hostname* | **port** *port* } | **reservation** | **server-identity-check** | **transport** | **url** { *url* | **cslu** *cslu_or_on-prem_url* | **default** | **smart** *smart_url* | **utility** *secondary_url* } | **usage** { **customer-tags** { **tag1** | **tag2** | **tag3** | **tag4** } *tag_value* | **interval** *interval_in_days* } | **utility** [**customer_info** { **city** *city* | **country** *country* | **postalcode** *postalcode* | **state** *state* | **street** *street* }] }

Syntax Description

custom_id *ID*	Although available on the CLI, this option is not supported.
enable	Although visible on the CLI, configuring this keyword has no effect. Smart licensing is always enabled.

privacy { **all** | **hostname** | **version** }	Sets a privacy flag to prevent the sending of the specified data privacy related information. When the flag is disabled, the corresponding information is sent in a message or offline file created by the product instance. Depending on the topology this is sent to one or more components, including CSSM, CSLU, and SSM On-Prem. *All data privacy settings are disabled by default*. You must configure the option you want to exclude from all communication: • **all**: All data privacy related information is excluded from any communication. The **no** form of the command causes all data privacy related information to be sent in a message or offline file. **Note** The Product ID (PID) and serial number are *included in the RUM report* regardless of whether data privacy is enabled or not. • **hostname**: Excludes hostname information from any communication. When hostname privacy is enabled, the *UDI* of the product instance is displayed on the applicable user interfaces (CSSM, CSLU, and SSM On-Prem). The **no** form of the command causes hostname information to be sent in a message or offline file. The hostname is displayed on the applicable user interfaces (CSSM, CSLU, and SSM On-Prem). • **version**: Excludes the Cisco IOS-XE software version running on the product instance and the Smart Agent version from any communication. The **no** form of the command causes version information to be sent in a message or offline file.

proxy { **address** *address_hostname* | **port** *port* }	Configures a proxy for license usage synchronization with CSLU or CSSM. This means that you can use this option to configure a proxy only if the transport mode is **license smart transport smart** (CSSM), or **license smart transport cslu** (CSLU). However, you cannot configure a proxy for license usage synchronization in an SSM On-Prem deployment, which also uses **license smart transport cslu** as the transport mode. Configure the following options: • **address** *address_hostname*: Configures the proxy address. For *address_hostname*, enter the enter the IP address or hostname of the proxy. • **port***port*: Configures the proxy port. For *port*, enter the proxy port number.
reservation	Enables or disables a license reservation feature. **Note** Although available on the CLI, this option is not applicable because license *reservation* is not applicable in the Smart Licensing Using Policy environment.
server-identity-check	Enables or disables the HTTP secure server identity check.
transport { **automatic** | **callhome** | **cslu** | **off** | **smart** }	Configures the mode of transport the product instance uses to communicate with CSSM. Choose from the following options: • **automatic**: Sets the transport mode **cslu**. **Note** The **automatic** keyword is not supported on Cisco Catalyst Wireless Controllers. • **callhome**: Enables Call Home as the transport mode. • **cslu**: Enables CSLU as the transport mode. This is the default transport mode. The same keyword applies to both CSLU *and* SSM On-Prem, but the URLs are different. See **cslu***cslu_or_on-prem_url* in the following row. • **off**: Disables all communication from the product instance. • **smart**: Enables Smart transport.

url { *url* | **cslu** *cslu_url* | **default** | **smart** *smart_url* | **utility** *secondary_url* }

Sets URL that is used for the configured transport mode. Choose from the following options:

- *url*: If you have configured the transport mode as **callhome**, configure this option. Enter the CSSM URL exactly as follows:

  `https://ptesdc.cloudapps.cisco.com/its/service/oddce/`

  The **no license smart url** *url* command reverts to the default URL.

- **cslu** *cslu_or_on-prem_url*: If you have configured the transport mode as **cslu**, configure this option, with the URL for CSLU or SSM On-Prem, as applicable:

  - If you are using CSLU, enter the URL as follows:

    `http://<cslu_ip_or_host>:8182/cslu/v1/pi`

    For `<cslu_ip_or_host>`, enter the hostname or the IP address of the windows host where you have installed CSLU. 8182 is the port number and it is the only port number that CSLU uses.

    The **no license smart url cslu** *cslu_or_on-prem_url* command reverts to `http://cslu-local:8182/cslu/v1/pi`

  - If you are using SSM On-Prem, enter the URL as follows:

    `http://<ip>/cslu/v1/pi/<tenant ID>`

    For <ip>, enter the hostname or the IP address of the server where you have installed SSM On-Prem. The <tenantID> must be the default local virtual account ID.

    Tip
    You can retrieve the entire URL from SSM On-Prem. In the software configuration guide (17.3.x and later), see Smart Licensing Using Policy > Task Library for Smart Licensing Using Policy > Retrieving the Transport URL (SSM On-Prem UI).

    The **no license smart url cslu** *cslu_or_on-prem_url* command reverts to `http://cslu-local:8182/cslu/v1/pi`

- **default**: Depends on the configured transport mode. Only the **smart** and **cslu** transport modes are supported with this option.

  If the transport mode is set to **cslu**, and you configure **license smart url default**, the CSLU URL is configured automatically

(`https://cslu-local:8182/cslu/v1/pi`).

If the transport mode is set to **smart**, and you configure **license smart url default**, the Smart URL is configured automatically (`https://smartreceiver.cisco.com/licservice/license`).

- **smart** *smart_url*: If you have configured the transport type as **smart**, configure this option. Enter the URL exactly as follows:

  `https://smartreceiver.cisco.com/licservice/license`

  When you configure this option, the system automatically creates a duplicate of the URL in **license smart url** *url*. You can ignore the duplicate entry, no further action is required.

  The **no license smart url smart***smart_url* command reverts to the default URL.

- **utility** *smart_url*: Although available on the CLI, this option is not supported.

usage { **customer-tags** { **tag1** | **tag2** | **tag3** | **tag4** } *tag_value* | **interval** *interval_in_days* }	Configures usage reporting settings. You can set the following options: • **customer-tags** { **tag1** | **tag2** | **tag3** | **tag4** } *tag_value*: Defines strings for inclusion in data models, for telemetry. Up to 4 strings (or tags) may be defined. For *tag_value*, enter the string value for each tag that you define. • **interval** *interval_in_days*: Sets the reporting interval in days. By default the RUM report is sent every 30 days. The valid value range is 1 to 3650. If you set the value to zero, RUM reports are not sent, regardless of what the applied policy specifies - this applies to topologies where CSLU or CSSM may be on the receiving end. If you set a value that is greater than zero and the transport type is set to **off**, then, between the *interval_in_days* and the policy value for `Ongoing reporting frequency(days):`, the lower of the two values is applied. For example, if *interval_in_days* is set to 100, and the value in the in the policy says `Ongoing reporting frequency (days):90`, RUM reports are sent every 90 days. If you do not set an interval, and the default is effective, the reporting interval is determined entirely by the policy value. For example, if the default value is effective and only unenforced licenses are in use, if the policy states that reporting is not required, then RUM reports are not sent.
utility [**customer_info** { **city** *city* | **country** *country* | **postalcode** *postalcode* | **state** *state* | **street** *street* }]	Although visible on the CLI, this option is not supported.

Command Default

Cisco IOS XE Amsterdam 17.3.1 or earlier: Smart Licensing is enabled by default.

Cisco IOS XE Amsterdam 17.3.2a and later: Smart Licensing Using Policy is enabled by default.

Command Modes

Global config (config)

Command History

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

Release	Modification
Cisco IOS XE Amsterdam 17.3.2a	The following keywords and variables were introduced with Smart Licensing Using Policy: • Under the **url**keyword, these options were introduced: { **cslu** *cslu_url* | **smart** *smart_url* } • Under the **transport** keyword, these options were introduced: { **cslu** | **off** } Further, the default transport type was changed from **callhome**, to **cslu**. • **usage** { **customer-tags** { **tag1** | **tag2** | **tag3** | **tag4** } *tag_value* | **interval** *interval_in_days* } The following keywords and variables under the **license smart** command are deprecated and no longer available on the CLI: **enable**and **conversion automatic**.
Cisco IOS XE Amsterdam 17.3.3	SSM On-Prem support was introduced. For product instance-initiated communication in an SSM On-Prem deployment, the existing [**no**]**license smart url cslu***cslu_or_on-prem_url* command supports the configuration of a URL for SSM On-Prem as well. But the required URL format for SSM On-Prem is: `http://<ip>/cslu/v1/pi/<tenant ID>`. The corresponding transport mode that must be configured is also an existing command (**license smart transport cslu**).
Cisco IOS XE Cupertino 17.9.1	• A new mechanism to send all data privacy related information was introduced. This information is no longer included in a RUM report. If data privacy is disabled (**no license smart privacy** {**all** | **hostname** | **version**} global configuration command), data privacy related information is sent in a separate sync message or offline file. • Support for sending hostname information was introduced. If the privacy setting for the hostname is disabled (**no license smart privacy hostname** global configuration command), hostname information is sent from the product instance, in a separate sync message, or offline file. Depending on the topology you have implemented, the hostname information is received by CSSM, CSLU, or SSM On-Prem. It is also displayed on the corresponding user interface.

Usage Guidelines

Data Privacy Settings

When you disable a privacy setting, the topology you have implemented determines the recipient and how the information reaches its destination:

- The recipient of the information may be one or more of the following: CSSM, CSLU, and SSM On-Prem. The privacy setting has no effect on a controller (Cisco DNA Center).

In case of the **hostname** keyword, after the hostname information is received by CSSM, CSLU, or SSM On-Prem, it is also displayed on the corresponding UIs – as applicable. If you then *enable* privacy the corresponding UIs revert to displaying the UDI of the product instance.

- How the information is sent.
  - In case of a topology where the product instance initiates communication, the product instance initiates the sending of this information in a message, to CSSM, or CSLU, or SSM On-Prem.

    The product instance sends the hostname sent every time one of the following events occur: the product instance boots up, the hostname changes, there is a switchover in a High Availability set-up.
  - In case of a topology where CSLU or SSM On-Prem initiate communication, the corresponding component initiates the retrieval of privacy information from the product instance.

    The hostname is retrieved at the frequency you configure in CSLU or SSM On-Prem, to retrieve information.
  - In case of a topology where the product instance is in an air-gapped network, privacy information is included in the offline file that is generated when you enter the **license smart save usage** privileged EXEC command.

Note For all topologies, data privacy related information is *not* included in the RUM report.

Data privacy related information it is not stored by the product instance *prior* to sending or saving. This ensures that if and when information is sent, it is consistent with the data privacy setting at the time of sending or saving.

Communication failures and reporting

The reporting interval that you configure (**license smart usage interval** *interval_in_days* command), determines the date and time at which the product instance sends out the RUM report. If the scheduled interval coincides with a communication failure, the product instance attempts to send out the RUM report for up to four hours after the scheduled time has expired. If it is still unable to send out the report (because the communication failure persists), the system resets the interval to 15 minutes. Once the communication failure is resolved, the system reverts the reporting interval to the value that you last configured.

The system message you may see in case of a communicatin failure is %SMART_LIC-3-COMM_FAILED. For information about resolving this error and restoring the reporting interval value, in the software configuration guide of the required release (17.3.x onwards), see *System Configuration* > *Smart Licensing Using Policy* > *Troubleshooting Smart Licensing Using Policy*.

Examples

- Examples for Data Privacy, on page 96
- Examples for Transport Type and URL, on page 96
- Examples for Usage Reporting Options, on page 97

Examples for Data Privacy

The following examples show how to configure data privacy related information using **license smart privacy** command in global configuration mode. The accompanying **show license status** output displays configured information.

Note The output of the **show** command only tells you if a particular option is enabled or disabled.

Here, no data privacy related information information is sent:

```
Device#configure terminal
Device(config)#license smart privacy all
Device(config)#exit
Device#show license status
<output truncated>
Data Privacy:
 Sending Hostname: no
   Callhome hostname privacy: ENABLED
   Smart Licensing hostname privacy: ENABLED
 Version privacy: ENABLED

Transport:
 Type: Callhome
<output truncated>
```

Examples for Transport Type and URL

The following examples show how to configure some of the transport types using the **license smart transport** and the **license smart url** commands in global configuration mode. The accompanying **show license all** output displays configured information.

Transport **cslu**:

```
Device#configure terminal
Device(config)#license smart transport cslu
Device(config)#license smart url default
Device(config)#exit
Device#show license all
<output truncated>
Transport:
 Type: cslu
 Cslu address: http://192.168.0.1:8182/cslu/v1/pi
 Proxy:
   Not Configured
<output truncated>
```

Transport **smart**:

```
Device#configure terminal
Device(config)#license smart transport smart
Device(config)#license smart url smart https://smartreceiver.cisco.com/licservice/license
Device(config)#exit
Device#show license all
<output truncated>
Transport:
```

```
 Type: Smart
 URL: https://smartreceiver-stage.cisco.com/licservice/license
 Proxy:
   Not Configured
<output truncated>
```

Examples for Usage Reporting Options

The following examples show how to configure some of the usage reporting settings using the **license smart usage** command in global configuration mode. The accompanying **show running-config** output displays configured information.

Configuring the **customer-tag** option:

```
Device# configure terminal
Device(config)# license smart usage customer-tags tag1 SA/VA:01
Device(config)# exit
Device#show running-config | include tag1
license smart usage customer-tags tag1 SA/VA:01
```

Configuring a narrower reporting interval than the currently applied policy:

```
Device#show license status
<output truncated>
Usage Reporting:
Last ACK received: Sep 22 13:49:38 2020 PST
Next ACK deadline: Dec 21 12:02:21 2020 PST
 Reporting push interval: 30 days
Next ACK push check: Sep 22 12:20:34 2020 PST
 Next report push: Oct 22 12:05:43 2020 PST
Last report push: Sep 22 12:05:43 2020 PST
Last report file write: <none>
<output truncated>

Device#configure terminal
Device(config)#license smart usage interval 20
Device(config)#exit
Device#show license status
<output truncated>

Usage Reporting:
Last ACK received: Sep 22 13:49:38 2020 PST
 Next ACK deadline: Nov 22 12:02:21 2020 PST
Reporting push interval: 20 days
Next ACK push check: Sep 22 12:20:34 2020 PST
 Next report push: Oct 12 12:05:43 2020 PST
Last report push: Sep 22 12:05:43 2020 PST
Last report file write: <none>
<output truncated>
```

license smart (privileged EXEC)

To configure licensing functions such as requesting or returning authorization codes, saving Resource Utilization Measurement reports (RUM reports), importing a file on to a product instance, establishing trust with Cisco Smart Software Manager (CSSM), synchronizing the product instance with CSSM, or Cisco Smart License Utility (CSLU), or Smart Software Manager On-Prem (SSM On-Prem), and removing licensing information from the product instance, enter the **license smart** command in privileged EXEC mode with the corresponding keyword or argument.

license smart { **authorization** { **request** { **add** | **replace** } *feature_name* { **all** | **local** } | **return** { **all** | **local** } { **offline** [*filepath_filename*] | **online** } } | **clear eventlog** | **export return** { **all** | **local** } *feature_name* | **factory reset** | **import** *filepath_filename* | **save** { **trust-request** *filepath_filename* | **usage** { **all** | **days** *days* | **rum-id** *rum-ID* | **unreported** } { **file** *filepath_filename* } } | **sync** { **all** | **local** } | **trust idtoken** *id_token_value* { **local** | **all** } [**force**] }

Syntax Description

smart	Provides options for Smart Licensing.
authorization	Provides the option to request for, or return, authorization codes. Authorization codes are required *only* if you use licenses with enforcement type: export-controlled or enfored.
request	Requests an authorization code from CSSM, CSLU (CSLU in-turn fetches it from CSSM), or SSM On-Prem and installs it on the product instance.
add	Adds the requested license to the existing authorization code. The new authorization code will contain all the licenses of the existing authorization code and the requested license.
replace	Replaces the existing authorization code. The new authorization code will contain only the requested license. All licenses in the current authorization code are returned. When you enter this option, the product instance verifies if licenses that correspond to the authorization codes that will be removed, are in-use. If licenses are being used, an error message tells you to first disable the corresponding features.
feature_name	Name of the license for which you are requesting an authorization code.
all	Performs the action for all product instances in a High Availability configuration.
local	Performs the action for the *active* product instance. This is the default option.
return	Returns an authorization code back to the license pool in CSSM.
offline *filepath_filename*	Means the product instance is not connected to CSSM. The authorization code is returned offline. This option requires you to print the return code to a file. Optionally, you can also specify a path to save the file. The file format can be any readable format, such as `.txt` If you choose the offline option, you must complete the additional step of copying the return code from the CLI or the saved file and entering it in CSSM.

online	Means that the product instance is in a connected mode. The authorization code is returned to CSLU or CSSM directly.
clear eventlog	Clears all event log files from the product instance.
export return	Returns the authorization key for an export-controlled license.
factory reset	Clears all saved licensing information from the product instance.
import *filepath_filename*	Imports a file on to the product instance. The file may be that of an authorization code, a trust code, or, or a policy. For *filepath_filename*, specify the location, including the filename.
save	Provides options to save RUM reports or trust code requests.
trust-request *filepath_filename*	Saves the trust code request for the active product instance in the specified location. For *filepath_filename*, specify the absolute path to the file, including the filename.
usage { **all** | **days** *days* | **rum-id** *rum-ID* | **unreported** } { **file** *file_path* }	Saves RUM reports (license usage information) in the specified location. You must specify one of these options: • **all**: Saves all RUM reports. • **days** *days*: Saves RUM report for the last *n* number of days (excluding the current day). Enter a number. The valid range is 0 to 4294967295. For example, if you enter 3, RUM reports of the last three days are saved. • **rum-Id** *rum-ID*: Saves a specified RUM ID. The valid value range is 0 to 18446744073709551615. • **unreported**: Saves all unreported RUM reports. **file** *filepath_filename*: Saves the specified usage information to a file. Specify the absolute path to the file, including the filename.
sync { **all** | **local** }	Synchronizes with CSSM or CSLU, or SSM On-Prem, to send and receive any pending data. This includes uploading pending RUM reports, downloading the ACK response, any pending authorization codes, trust codes, and policies for the product instance. Specify the product instance by entering one of these options: • **all**: Performs synchronization for all the product instances in a High Availability set-up. If you choose this option, the product instance also sends the list of all the UDIs in the synchronization request. • **local**: Performs synchronization only for the active product instance sending the request, that is, its own UDI. This is the default option.
trust idtoken *id_token_value*	Establishes a trusted connection with CSSM. To use this option, you must first generate a token in the CSSM portal. Provide the generated token value for *id_token_value*.

force	Submits a trust code request even if a trust code already exists on the product instance. A trust code is node-locked to the UDI of a product instance. If the UDI is already registered, CSSM does not allow a new registration for the same UDI. Entering the **force** keyword overrides this behavior.

Command Default

Cisco IOS XE Amsterdam 17.3.1 or earlier: Smart Licensing is enabled by default.

Cisco IOS XE Amsterdam 17.3.2a and later: Smart Licensing Using Policy is enabled by default.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2a	The following keywords and variables were introduced with Smart Licensing Using Policy: • **authorization** { **request** { **add** | **replace** } *feature_name* { **all** | **local** } | **return** { **all** | **local** } { **offline** [*path*] | **online** } } • **import** *file_path* • **save** { **trust-request** *filepath_filename* | **usage** { **all** | **days** *days* | **rum-id** *rum-ID* | **unreported** } { **file** *file_path* } } • **sync** { **all** | **local** } • **trust idtoken** *id_token_value* { **local** | **all** } [**force**] The following keywords and variables under the **license smart** command are deprecated and no longer available on the CLI: • **register idtoken** *token_id* [**force**] • **renew id** { **ID** | **auth** } • **debug** { **error** | **debug** | **trace** | **all** } • **reservation** { **cancel** [**all** | **local**] | **install** [**file**] *key* | **request** { **all** | **local** | **universal** } | **return** [**all** | **authorization** { *auth_code* | **file** *filename* } | **Local**] *key* } • **mfg reservation** { **request** | **install** | **install file** | **cancel** } • **conversion** { **start** | **stop** }
Cisco IOS XE Amsterdam 17.3.3	Support for SSM On-Prem was introduced. You can perform licensing-related tasks such as saving Resource Utilization Measurement reports (RUM reports), importing a file on to a product instance, synchronizing the product instance, returning authorization codes, and removing licensing information from the product instance in an SSM On-Prem deployment.

Usage Guidelines

Overwriting a Trust Code

Use case for the **force** option when configuring the **license smart trust idtoken** command: You use same token for all the product instances that are part of one Virtual Account. If the product instance has moved from one account to another (for instance, because it was added to a High Availability set-up, which is part of another Virtual Account), then there may be an existing trust code you have to overwrite.

Removing Licensing Information

Entering the **licence smart factory reset** command removes all licensing information (except the licenses in-use) from the product instance, including any authorization codes, RUM reports etc. Therefore, we recommend the use of this command only if the product instance is being returned (Return Material Authrization, or RMA), or being decommissioned permanently. We also recommend that you send a RUM report to CSSM, before you remove licensing information from the product instance - this is to ensure that CSSM has up-to-date usage information.

Authorization Codes and License Reservations:

Options relating to authorization codes and license reservations:

- Since there are no export-controlled or enforced licenses on any of the Cisco Catalyst Wireless Controllers, and the notion of reserved licenses is not applicable in the Smart Licensing Using Policy environment, the following commands are not applicable:
  - { { **license smart authorization request** { **add** | **replace** | **save** *path* } *feature_name* { **all** | **local** } *request_count* } }
  - **license smart export return**
- The following option is applicable and required for any SLR authorization codes you may want to return:

  license smart authorization return { **all** | **local** } { **offline** [*path*] | **online** }

Examples

- Example for Saving Licensing Usage Information, on page 101
- Example for Installing a Trust Code, on page 102
- Example for Returning an SLR Authorization Code, on page 102

Example for Saving Licensing Usage Information

The following example shows how you can save license usage information on the product instance. You can use this option to fulfil reporting requirements in an air-gapped network. In the example, the file is first save to flash memory and then copied to a TFTP location:

```
 Device> enable
Device# license smart save usage unreported file flash:RUM-unrep.txt
Device# dir
Directory of bootflash:/

33      -rw-             5994   Nov 2 2020 03:58:04 +05:00  RUM-unrep.txt

Device# copy flash:RUM-unrep.txt tftp://192.168.0.1//auto/tftp-user/user01/
Address or name of remote host [192.168.0.1]?
Destination filename [//auto/tftp-user/user01/RUM-unrep.txt]?
```

```
!!
15128 bytes copied in 0.161 secs (93963 bytes/sec)
```

After you save RUM reports to a file, you must upload it to CSSM (from a workstation that has connectivity to the internet, and Cisco).

Example for Installing a Trust Code

The following example shows how to install a trust code even if one is already installed on the product instance. This requires connectivity to CSSM. The accompanying **show license status** output shows sample output after successful installation:

Before you can install a trust code, you must generate a token and download the corresponding file from CSSM.

Use the **show license status** command (`Trust Code Installed:`) to verify results.

```
Device> enable
Device# license smart trust idtoken
NGMwMjk5mYtNZaxMS00NzMZmtgWm local force

Device# show license status
<output truncated>
Trust Code Installed:
  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
    INSTALLED on Nov 02 05:19:05 2020 IST
  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
    INSTALLED on Nov 02 05:19:05 2020 IST
<output truncated>
```

Example for Returning an SLR Authorization Code

The following example shows how to remove and return an SLR authorization code. Here the code is returned offline (no connectivity to CSSM). The accompanying **show license all** output shows sample output after successful return:

```
Device> enable
Device# show license all
<output truncated>
License Authorizations
======================
Overall status:
  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
      Status: SPECIFIC INSTALLED on Nov 02 03:16:01 2020 IST
      Last Confirmation code: 102fc949
  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
      Status: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
      Last Confirmation code: ad4382fe
<output truncated>

Device# license smart authorization return local offlline
Enter this return code in Cisco Smart Software Manager portal:
UDI: PID:C9800-CL-K9,SN:93BBAH93MGS
    Return code: CqaUPW-WSPYiq-ZNU2ci-SnWydS-hBCXHP-MuyPqy-PJ1GiG-tPTGQj-S2h
UDI: PID:C9800-CL-K9,SN:9XECPSUU4XN
    Return code: CNLwxR-eWiAEJ-XaTEQg-j4rrYW-dSRz9j-37VpcP-imjuLD-mNeA4k-TXA

Device# show license all
<output truncated>
```

```
License Authorizations
======================
Overall status:
  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
      Status: NOT INSTALLED
      Last return code: CqaUPW-WSPYiq-ZNU2ci-SnWydS-hBCXHP-MuyPqy-PJ1GiG-tPTGQj-S2h
  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
      Status: NOT INSTALLED
      Last return code: CNLwxR-eWiAEJ-XaTEQg-j4rrYW-dSRz9j-37VpcP-imjuLD-mNeA4k-TXA
<output truncated>
```

If you choose the **offline** option, you must complete the additional step of copying the return code from the CLI or the saved file and entering it in CSSM.

line vty

To identify a specific line for configuration and begin the command in line configuration mode in a virtual terminal for remote console access, use the **line vty** command.

line vty *line_number*

Syntax Description

line_number	First line number. Valid values range from 0 to 530.

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 identify a specific line for configuration in a virtual terminal:

```
Device# line vty 10
```

local-auth ap eap-fast

To configure Flex policy local authentication using EAP Fast method, use the **local-auth ap eap-fast** command.

local-auth ap eap-fast *profile-name*

Syntax Description

profile-name	Enter eap-fast profile name.

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 EAP Fast method authentication on a Flex policy:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile flex profile-name
Device(config-wireless-flex-profile)# local-auth ap eap-fast eap-fast-profile-name
```

local-site

To configure the site as local site, use the **local-site** command.

local-site

Syntax Description

local-site	Configure this site as local site.

Command Default

None

Command Modes

config-site-tag

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 current site as local site:

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

location expiry

To configure the location expiry duration, use the **location expiry** command in global configuration mode.

location expiry {**calibrating-client** | **client** | **tags** } *timeout-duration*

Syntax Description

calibrating-client	Timeout value for calibrating clients.
client	Timeout value for clients.
tags	Timeout value for RFID tags.
timeout-duration	Timeout duration, in seconds.

Command Default

Timeout value is not configured.

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 the location expiry duration:

```
Device(config)# location expiry tags 50
```

location notify-threshold

To configure the NMSP notification threshold for RSSI measurements, use the **location notify-threshold** command in global configuration mode. To remove the NMSP notification threshold for RSSI measurements, use the **no** form of this command.

location notify-threshold {**client** | **rogue-aps** | **tags** } *db*
no location notify-threshold {**client** | **rogue-aps** | **tags** }

Syntax Description

client	Specifies the NMSP notification threshold (in dB) for clients and rogue clients. The valid range for the threshold parameter is 0 to 10 dB, and the default value is 0 dB.
rogue-aps	Specifies the NMSP notification threshold (in dB) for rogue access points. The valid range for the threshold parameter is 0 to 10 dB, and the default value is 0 dB.
tags	Specifies the NMSP notification threshold (in dB) for RFID tags. The valid range for the threshold parameter is 0 to 10 dB, and the default value is 0 dB.
db	The valid range for the threshold parameter is 0 to 10 dB, and the default value is 0 dB.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1 Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

This example shows how to configure the NMSP notification threshold to 10 dB for clients. A notification NMSP message is sent to MSE as soon as the client RSSI changes by 10 dB:

```
Device# configure terminal
Device(config)# location notify-threshold client 10
Device(config)# end
```

log-export-mode

To configure the log export using FTP, STP and TFTP, use the **log-export-mode** command. Use the **no** command to negate the command or to set the command to its default.

log-export-mode { **ftp** | **stp** | **tftp** }

no log-export-mode { **ftp** | **stp** | **tftp** }

Syntax Description

ftp	Configures the log export using FTP.
stp	Configures the log export using STP.
tftp	Configures the log export using TFTP.

Command Default

None

Command Modes

Wireless trace export profile configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

```
Device(config)# wireless profile transfer trace-export trace-export-name
Device(config-wireless-trace-export-profile)# log-export-mode tftp
```

login authentication

To configure login authentication parameters, use the **login authentication** command.

login authentication *word* **default**

Syntax Description

word	Authentication list with a name.
default	Uses the default authentication list.

Command Default

None

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.

Examples

The following example shows how to configure login authentication :

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# line console 0
Device(config-line)# login authentication NO_LOGIN
```

login block-for

To configure the login security on the Cisco controller and to set the duration for which the controller has to block further login attempts after a specified number of consecutive failed login attempts within a certain time frame, use the **login block-for** command.

login block-for *duration* **attempts** *attempts* **within** *time-frame*

Syntax Description

duration	Specifies the duration in seconds for which the device will block login attempts
attempts	Number of consecutive failed login attempts
attempts	Specifies the maximum number of failed attempts
within	Time frame within which the specified number of consecutive failed login attempts must occur to trigger the blocking
time-frame	Specifies the time period in seconds

Command Default

None

Command Modes

Global 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 the login security on the controller to set the duration of 60 seconds for which the controller has to block further login attempts after 3 unsuccessful login attempts within a period of 10 seconds.:

```
Device# login block-for 60 attempts 3 within 10
```

mac-filtering

To enable MAC filtering on a WLAN, use the **mac-filtering** command.

mac-filtering [*mac-authorization-list*]

Syntax Description

mac-authorization-list	Name of the Authorization list.

Command Default

None

Command Modes

config-wlan

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 MAC filtering on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan-name wlan-index SSID-name
Device(config-wlan)# mac-filtering
```

mab request format attribute

To configure the delimiter while configuring MAC filtering on a WLAN, use the **mab request format attribute** command in global configuration mode. To disable the delimiter while configuring MAC filtering on a WLAN, use the **no** form of this command.

mab request format attribute { **1 groupsize** *size* **separator** *separator* [**lowercase** | **uppercase**] | **2** { **0** | **7** | **LINE** } **LINE** *password* | **32 vlan access-vlan** }

no mab request format attribute { **1 groupsize** *size* **separator** *separator* [**lowercase** | **uppercase**] | **2** { **0** | **7** | **LINE** } **LINE** *password* | **32 vlan access-vlan** }

Syntax Description

1	Specifies the username format used for MAB requests.
groupsize *size*	Specifies the number of hex digits per group. The valid values range from 1 to 12.
separator *separator*	Specifies how to separate groups. The separators are hyphen (-), colon (:), and full stop (.) For more information about the groupsize and separator, refer to the Overview of the Configurable MAB Username and Password.
lowercase	Specifies the username in lowercase format.
uppercase	Specifies the username in uppercase format.
2	Specifies the global password used for all the MAB requests.
0	Specifies the unencrypted password.
7	Specifies the hidden password.
LINE	Specifies the encrypted or unencrypted password.
password	LINE password.
32	Specifies the NAS-Identifier attribute.
vlan	Specifies a VLAN.
access-vlan	Specifies the configured access VLAN.

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.

Example:

The following example shows how to configure the delimiter while configuring MAC filtering:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# mab request format attribute 1 groupsize 4 separator -
```

mbo

To configure WiFi Alliance Agile Multiband (MBO) on WLAN, use the **mbo** command.

mbo

Syntax Description This command has no arguments or keywords.

Command Default MBO is not enabled.

Command Modes WLAN configuration

Command History

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

Usage Guidelines

This example shows how to configure WiFi Alliance Agile Multiband (MBO) on WLAN:

```
Device# configure terminal
Device(config)# wlan wlan-demo 1 ssid-demo
Device(config-wlan)# mbo
Device(config-wlan)# end
```

Note If you use WPA2 WLAN while configuring MBO for WLAN, you need to enable PMF in your configuration.

match (access-map configuration)

To set the VLAN map to match packets against one or more access lists, use the **match** command in access-map configuration mode on the switch stack or on a standalone switch. To remove the match parameters, use the **no** form of this command.

match { **ip address** { *name number* } [*name number*] [*name number*] . . . | **ipv6 address** { *name number* } [*name number*] [*name number*] . . . | **mac address** { *name* } [*name*] [*name*] . . . }
no match { **ip address** { *name number* } [*name number*] [*name number*] . . . | **ipv6 address** { *name number* } [*name number*] [*name number*] . . . | **mac address** { *name* } [*name*] [*name*] . . . }

Syntax Description

ip address	Sets the access map to match packets against an IP address access list.
ipv6 address	Sets the access map to match packets against an IPv6 address access list.
mac address	Sets the access map to match packets against a MAC address access list.
name	Name of the access list to match packets against.
number	Number of the access list to match packets against. This option is not valid for MAC access lists.

Command Default

The default action is to have no match parameters applied to a VLAN map.

Command Modes

Access-map configuration

Command History

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

Usage Guidelines

You enter access-map configuration mode by using the **vlan access-map** global configuration command.

You must enter one access list name or number; others are optional. You can match packets against one or more access lists. Matching any of the lists counts as a match of the entry.

In access-map configuration mode, use the **match** command to define the match conditions for a VLAN map applied to a VLAN. Use the **action** command to set the action that occurs when the packet matches the conditions.

Packets are matched only against access lists of the same protocol type; IP packets are matched against IP access lists, IPv6 packets are matched against IPv6 access lists, and all other packets are matched against MAC access lists.

IP, IPv6, and MAC addresses can be specified for the same map entry.

This example shows how to define and apply a VLAN access map vmap4 to VLANs 5 and 6 that will cause the interface to drop an IP packet if the packet matches the conditions defined in access list al2:

```
Device(config)# vlan access-map vmap4
Device(config-access-map)# match ip address al2
Device(config-access-map)# action drop
Device(config-access-map)# exit
Device(config)# vlan filter vmap4 vlan-list 5-6
```

You can verify your settings by entering the **show vlan access-map** privileged EXEC command.

match activated-service-template

To create a condition that evaluates true based on the service template activated on a session, use the **match activated-service-template** command in control class-map filter configuration mode. To create a condition that evaluates true if the service template activated on a session does not match the specified template, use the **no-match activated-service-template** command in control class-map filter configuration mode. To remove the condition, use the **no** form of this command.

match activated-service-template *template-name*
no-match activated-service-template *template-name*
no {**match** | **no-match**} **activated-service-template** *template-name*

Syntax Description

template-name	Name of a configured service template as defined by the **service-template** command.

Command Default

The control class does not contain a condition based on the service template.

Command Modes

Control class-map filter configuration (config-filter-control-classmap)

Command History

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

Usage Guidelines

The **match activated-service-template** command configures a match condition in a control class based on the service template applied to a session. A control class can contain multiple conditions, each of which will evaluate as either true or false. The control class defines whether all, any, or none of the conditions must evaluate true for the actions of the control policy to be executed.

The **no-match** form of this command specifies a value that results in an unsuccessful match. All other values of the specified match criterion result in a successful match. For example, if you configure the **no-match activated-service-template SVC_1** command, all template values except SVC_1 are accepted as a successful match.

The **class** command associates a control class with a control policy.

Examples

The following example shows how to configure a control class that evaluates true if the service template named VLAN_1 is activated on the session:

```
class-map type control subscriber match-all CLASS_1
 match activated-service-template VLAN_1
```

Related Commands

Command	Description
activate (policy-map action)	Activates a control policy or service template on a subscriber session.
class	Associates a control class with one or more actions in a control policy.
match service-template	Creates a condition that evaluates true based on an event's service template.

Command	Description
service-template	Defines a template that contains a set of service policy attributes to apply to subscriber sessions.

match any

To perform a match on any protocol that passes through the device, use the **match any** command.

match any

Command Default None

Command Modes config-cmap

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 match any packet passing through the device:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# class-map cmap-name
Device(config-cmap)# match any
```

match day

To perform a match using day, days, or a generic grouping of days (weekends or weekdays), use the **match day** command.

match day *day-string*

Command Default None

Command Modes Filter Control Classmap Configuration (config-filter-control-classmap)

Command History

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

Usage Guidelines You should also disable AAA override for this command to work.

Examples

The following example shows how to perform a match using day:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# class-map type control subscriber match-all class-map-name
Device(config-filter-control-classmap)# match day day-string
```

match device-type

To perform a match using device type, use the **match device-type** command.

match device-type*device-type*

Command Default None

Command Modes Filter Control Classmap Configuration (config-filter-control-classmap)

Command History

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

Usage Guidelines You should enable device classifier for the device list to be populated.

Examples

The following example shows how to perform a match using device type:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# class-map type control subscriber match-allclass-map-name
Device(config-filter-control-classmap)# match device-type device-type
```

match eap-type

To perform a match using Extensible Authentication Protocol (EAP), use the **match eap-type** command.

match eap-type {**fast** | **gtc** | **leap** | **md5** | **mschapv2** | **peap** | **tls**}

Syntax Description

fast	Flexible authentication through secure tunneling.
gtc	Generic token card.
leap	Lightweight extensible authentication protocol.
md5	MD5-tunneled authentication protocol.
mschapv2	MSCHAPV2 authentication mechanism.
peap	Protected extensible authentication protocol.
tls	Transport layer security.

Command Default

None

Command Modes

Filter Control Classmap Configuration (config-filter-control-classmap)

Command History

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

Usage Guidelines

You should also disable AAA override for this command to work.

Examples

The following example shows how to perform a match using the eap-type PEAP:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# class-map type control subscriber match-all class-map-name
Device(config-filter-control-classmap)# match eap-type  peap
```

match join-time-of-day

To perform a match using time of the day, use the **match join-time-of-day** command.

match join-time-of-day *start-time end-time*

Command Default None

Command Modes Filter Control Classmap Configuration (config-filter-control-classmap)

Command History

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

Usage Guidelines Join time is considered for matching. For example, if the match filter is set from 11:00 a.m. to 2:00 p.m., a device joining at 10:59 a.m. is not considered, even if it acquires credentials after 11:00 a.m.

You should also disable AAA override for the command to work.

Examples

The following example shows how to perform a match using the joining time:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# class-map type control subscriber match-all class-map-name
Device(config-filter-control-classmap)# match join-time-of-day start-time end-time
```

match message-type

To set a message type to match a service list, use the **match message-type** command.

match message-type {**announcement** | **any** | **query**}

Syntax Description

announcement	Allows only service advertisements or announcements for the Device.
any	Allows any match type.
query	Allows only a query from the client for a certain Device in the network.

Command Default

None

Command Modes

Service list configuration.

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

Multiple service maps of the same name with different sequence numbers can be created, and the evaluation of the filters will be ordered on the sequence number. Service lists are an ordered sequence of individual statements, with each one having a permit or deny result. The evaluation of a service list consists of a list scan in a predetermined order, and an evaluation of the criteria of each statement that matches. A list scan is stopped once the first statement match is found and a permit/deny action associated with the statement match is performed. The default action after scanning through the entire list is to deny.

Note It is not possible to use the **match** command if you have used the **service-list mdns-sd** *service-list-name* **query** command. The **match** command can be used only for the **permit** or **deny** option.

Example

The following example shows how to set the announcement message type to be matched:

```
Device(config-mdns-sd-sl)# match message-type announcement
```

match non-client-nrt

To match non-client NRT (non-real-time), use the **match non-client-nrt** command in class-map configuration mode. Use the **no** form of this command to return to the default setting.

match non-client-nrt
no match non-client-nrt

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Class-map

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1 Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

None

This example show how you can configure non-client NRT:

```
Device(config)# class-map test_1000
Device(config-cmap)# match non-client-nrt
```

match protocol

To configure the match criterion for a class map on the basis of a specified protocol, use the **match protocol** command in class-map configuration or policy inline configuration mode. To remove the protocol-based match criterion from the class map, use the **no** form of this command. For more information about the **match protocol** command, refer to the *Cisco IOS Quality of Service Solutions Command Reference*.

match protocol {*protocol-name* | **attribute category** *category-name* | **attribute sub-category** *sub-category-name* | **attribute application-group** *application-group-name*}

Syntax Description

protocol-name	Name of the protocol (for example, bgp) used as a matching criterion.
category-name	Name of the application category used as a matching criterion.
sub-category-name	Name of the application subcategory used as a matching criterion.
application-group-name	Name of the application group as a matching criterion. When the application name is specified, the application is configured as the match criterion instead of the application group.

Command Default

No match criterion is configured.

Command Modes

Class-map configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

This example shows how to create class maps with apply match protocol filters for application name, category, and sub category:

```
Device# configure terminal
Device(config)# class-map cat-browsing
Device(config-cmap)# match protocol attribute category browsing
Device(config-cmap)#end

Device# configure terminal
Device(config)# class-map cat-fileshare
Device(config-cmap)# match protocol attribute category file-sharing
Device(config-cmap)#end

Device# configure terminal
Device(config)# class-map match-any subcat-terminal
Device(config-cmap)# match protocol attribute sub-category terminal
Device(config-cmap)#end

Device# configure terminal
Device(config)# class-map match-any webex-meeting
Device(config-cmap)# match protocol webex-meeting
Device(config-cmap)#end
```

This example shows how to create policy maps and define existing class maps for upstream QoS:

```
Device# configure terminal
Device(config)# policy-map test-avc-up
Device(config-pmap)# class cat-browsing
Device(config-pmap-c)# police 150000
Device(config-pmap-c)# set dscp 12
Device(config-pmap-c)#end


Device# configure terminal
Device(config)# policy-map test-avc-up
Device(config-pmap)# class cat-fileshare
Device(config-pmap-c)# police 1000000
Device(config-pmap-c)# set dscp 20
Device(config-pmap-c)#end


Device# configure terminal
Device(config)# policy-map test-avc-up
Device(config-pmap)# class subcat-terminal
Device(config-pmap-c)# police 120000
Device(config-pmap-c)# set dscp 15
Device(config-pmap-c)#end

Device# configure terminal
Device(config)# policy-map test-avc-up
Device(config-pmap)# class webex-meeting
Device(config-pmap-c)# police 50000000
Device(config-pmap-c)# set dscp 21
Device(config-pmap-c)#end
```

This example shows how to create policy maps and define existing class maps for downstream QoS:

```
Device# configure terminal
Device(config)# policy-map test-avc-down
Device(config-pmap)# class cat-browsing
Device(config-pmap-c)# police 200000
Device(config-pmap-c)# set dscp 10
Device(config-pmap-c)#end


Device# configure terminal
Device(config)# policy-map test-avc-up
Device(config-pmap)# class cat-fileshare
Device(config-pmap-c)# police 300000
Device(config-pmap-c)# set wlan user-priority 2
Device(config-pmap-c)# set dscp 20
Device(config-pmap-c)#end


Device# configure terminal
Device(config)# policy-map test-avc-up
Device(config-pmap)# class subcat-terminal
Device(config-pmap-c)# police 100000
Device(config-pmap-c)# set dscp 25
Device(config-pmap-c)#end

Device# configure terminal
Device(config)# policy-map test-avc-up
Device(config-pmap)# class webex-meeting
Device(config-pmap-c)# police 60000000
```

```
Device(config-pmap-c)# set dscp 41
Device(config-pmap-c)#end
```

This example shows how to apply defined QoS policy on a WLAN:

```
Device# configure terminal
Device(config)#wlan  alpha
Device(config-wlan)#shut
Device(config-wlan)#end
Device(config-wlan)#service-policy client input test-avc-up
Device(config-wlan)#service-policy client output test-avc-down
Device(config-wlan)#no shut
Device(config-wlan)#end
```

match service-instance

To set a service instance to match a service list, use the **match service-instance** command.

match service-instance *line*

Syntax Description

line	Regular expression to match the service instance in packets.

Command Default

None

Command Modes

Service list configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

It is not possible to use the **match** command if you have used the **service-list mdns-sd** *service-list-name* **query** command. The **match** command can be used only for the **permit** or **deny** option.

Example

The following example shows how to set the service instance to match:

```
Device(config-mdns-sd-sl)# match service-instance servInst 1
```

match service-type

To set the value of the mDNS service type string to match, use the **match service-type** command.

match service-type *line*

Syntax Description

line	Regular expression to match the service type in packets.

Command Default

None

Command Modes

Service list configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

It is not possible to use the **match** command if you have used the **service-list mdns-sd** *service-list-name* **query** command. The **match** command can be used only for the **permit** or **deny** option.

Example

The following example shows how to set the value of the mDNS service type string to match:

```
Device(config-mdns-sd-sl)# match service-type _ipp._tcp
```

match user-role

To configure the class-map attribute filter criteria, use the **match user-role** command.

match user-role *user-role*

Command Default None

Command Modes config-filter-control-classmap

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 class-map attribute filter criteria:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# class-map type control subscriber match-any map-name
Device(config-filter-control-classmap)# match user-role user-role
```

match username

To create a condition that evaluates true based on an event's username, use the **match username** command in control class-map filter configuration mode. To create a condition that evaluates true if an event's username does not match the specified username, use the **no-match username** command in control class-map filter configuration mode. To remove the condition, use the **no** form of this command.

match username *username*
no-match username *username*
no {**match** | **no-match**} **username** *username*

Syntax Description

username	Username.

Command Default

The control class does not contain a condition based on the event's username.

Command Modes

Control class-map filter configuration (config-filter-control-classmap)

Command History

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

Usage Guidelines

The **match username** command configures a match condition in a control class based on the username. A control class can contain multiple conditions, each of which will evaluate as either true or false. The control class defines whether all, any, or none of the conditions must evaluate true to execute the actions of the control policy.

The **no-match** form of this command specifies a value that results in an unsuccessful match. All other values of the specified match criterion result in a successful match. For example, if you configure the **no-match username josmithe** command, the control class accepts any username value except josmithe as a successful match.

The **class** command associates a control class with a control policy.

Examples

The following example shows how to configure a control class that evaluates true if the username is josmithe:

```
class-map type control subscriber match-all CLASS_1
 match username josmithe
```

Related Commands

Command	Description
class	Associates a control class with one or more actions in a control policy.
policy-map type control subscriber	Defines a control policy for subscriber sessions

match (access-map configuration)

To set the VLAN map to match packets against one or more access lists, use the **match** command in access-map configuration mode. Use the **no** form of this command to remove the match parameters.

{**match ip address** {*namenumber*} [*namenumber*] [*namenumber*]**. . .** | **mac address** *name* [*name*] [*name*]**. . .**}
{**no match ip address** {*namenumber*} [*namenumber*] [*namenumber*]**. . .** | **mac address** *name* [*name*] [*name*]**. . .**}

Syntax Description

ip address	Set the access map to match packets against an IP address access list.
mac address	Set the access map to match packets against a MAC address access list.
name	Name of the access list to match packets against.
number	Number of the access list to match packets against. This option is not valid for MAC access lists.

Command Default

The default action is to have no match parameters applied to a VLAN map.

Command Modes

Access-map configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1 Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

You enter access-map configuration mode by using the **vlan access-map** global configuration command.

You must enter one access list name or number; others are optional. You can match packets against one or more access lists. Matching any of the lists counts as a match of the entry.

In access-map configuration mode, use the **match** command to define the match conditions for a VLAN map applied to a VLAN. Use the **action** command to set the action that occurs when the packet matches the conditions.

Packets are matched only against access lists of the same protocol type; IP packets are matched against IP access lists, and all other packets are matched against MAC access lists.

Both IP and MAC addresses can be specified for the same map entry.

Examples

This example shows how to define and apply a VLAN access map *vmap4* to VLANs 5 and 6 that will cause the interface to drop an IP packet if the packet matches the conditions defined in access list *al2*.

```
Device(config)# vlan access-map vmap4
Device(config-access-map)# match ip address al2
```

```
Device(config-access-map)# action drop
Device(config-access-map)# exit
Device(config)# vlan filter vmap4 vlan-list 5-6
```

You can verify your settings by entering the **show vlan access-map** privileged EXEC command.

match (class-map configuration)

To define the match criteria to classify traffic, use the **match** command in class-map configuration mode. Use the **no** form of this command to remove the match criteria.

Cisco IOS XE Everest 16.5.x and Earlier Releases

match {**access-group** {**name***acl-name acl-index*} | **class-map** *class-map-name* | **cos** *cos-value* | **dscp** *dscp-value* | [**ip**] **dscp** *dscp-list* | [**ip**] **precedence** *ip-precedence-list* | **precedence** *precedence-value1...value4* | **qos-group** *qos-group-value* | **vlan** *vlan-id*}
no match {**access-group** {**name***acl-name acl-index*} | **class-map** *class-map-name* | **cos** *cos-value* | **dscp** *dscp-value* | [**ip**] **dscp** *dscp-list* | [**ip**] **precedence** *ip-precedence-list* | **precedence** *precedence-value1...value4* | **qos-group** *qos-group-value* | **vlan** *vlan-id*}

Cisco IOS XE Everest 16.6.x and Later Releases

match {**access-group** {**name** *acl-name acl-index*} | **cos** *cos-value* | **dscp** *dscp-value* | [**ip**] **dscp** *dscp-list* | [**ip**] **precedence** *ip-precedence-list* | **mpls** *experimental-value* | **non-client-nrt** | **precedence** *precedence-value1...value4* | **protocol** *protocol-name* | **qos-group** *qos-group-value* | **vlan** *vlan-id* | **wlan** *wlan-id*}
no match {**access-group** {**name** *acl-name acl-index*} | **cos** *cos-value* | **dscp** *dscp-value* | [**ip**] **dscp** *dscp-list* | [**ip**] **precedence** *ip-precedence-list* | **mpls** *experimental-value* | **non-client-nrt** | **precedence** *precedence-value1...value4* | **protocol** *protocol-name* | **qos-group** *qos-group-value* | **vlan** *vlan-id* | **wlan** *wlan-id*}

Syntax Description

access-group	Specifies an access group.
name *acl-name*	Specifies the name of an IP standard or extended access control list (ACL) or MAC ACL.
acl-index	Specifies the number of an IP standard or extended access control list (ACL) or MAC ACL. For an IP standard ACL, the ACL index range is 1 to 99 and 1300 to 1999. For an IP extended ACL, the ACL index range is 100 to 199 and 2000 to 2699.
class-map *class-map-name*	Uses a traffic class as a classification policy and specifies a traffic class name to use as the match criterion. **Note** This command is not supported in Cisco IOS XE Everest 16.5.1a.
cos *cos-value*	Matches a packet on the basis of a Layer 2 class of service (CoS)/Inter-Switch Link (ISL) marking. The cos-value is from 0 to 7. You can specify up to four CoS values in one **match cos** statement, separated by a space.

dscp *dscp-value*	Specifies the parameters for each DSCP value. You can specify a value in the range 0 to 63 specifying the differentiated services code point value.
ip dscp *dscp-list*	Specifies a list of up to eight IP Differentiated Services Code Point (DSCP) values to match against incoming packets. Separate each value with a space. The range is 0 to 63. You also can enter a mnemonic name for a commonly used value.
ip precedence *ip-precedence-list*	Specifies a list of up to eight IP-precedence values to match against incoming packets. Separate each value with a space. The range is 0 to 7. You also can enter a mnemonic name for a commonly used value.
precedence *precedence-value1...value4*	Assigns an IP precedence value to the classified traffic. The range is 0 to 7. You also can enter a mnemonic name for a commonly used value.
qos-group *qos-group-value*	Identifies a specific QoS group value as a match criterion. The range is 0 to 31.
vlan *vlan-id*	Identifies a specific VLAN as a match criterion. The range is 1 to 4094.
mpls *experimental-value*	Specifies Multi Protocol Label Switching specific values.
non-client-nrt	Matches a non-client NRT (non-real-time).
protocol *protocol-name*	Specifies the type of protocol.
wlan *wlan-id*	Identifies 802.11 specific values.

Command Default

No match criteria are defined.

Command Modes

Class-map configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1 Cisco IOS XE Gibraltar 16.12.1	This command was introc

Usage Guidelines

The **match** command is used to specify which fields in the incoming packets are examined to classify the packets. Only the IP access group or the MAC access group matching to the Ether Type/Len are supported.

If you enter the **class-map match-any***class-map-name* global configuration command, you can enter the following **match** commands:

- **match access-group name** *acl-name*

Note The ACL must be an extended named ACL.

- **match ip dscp** *dscp-list*
- **match ip precedence** *ip-precedence-list*

The **match access-group** *acl-index* command is not supported.

To define packet classification on a physical-port basis, only one **match** command per class map is supported. In this situation, the **match-any** keyword is equivalent.

For the **match ip dscp** *dscp-list* or the **match ip precedence** *ip-precedence-list* command, you can enter a mnemonic name for a commonly used value. For example, you can enter the **match ip dscp af11** command, which is the same as entering the **match ip dscp 10** command. You can enter the **match ip precedence critical** command, which is the same as entering the **match ip precedence 5** command. For a list of supported mnemonics, enter the **match ip dscp ?** or the **match ip precedence ?** command to see the command-line help strings.

Use the **input-interface** *interface-id-list* keyword when you are configuring an interface-level class map in a hierarchical policy map. For the *interface-id-list*, you can specify up to six entries.

Examples

This example shows how to create a class map called class2, which matches all the incoming traffic with DSCP values of 10, 11, and 12:

```
Device(config)# class-map class2
Device(config-cmap)# match ip dscp 10 11 12
Device(config-cmap)# exit
```

This example shows how to create a class map called class3, which matches all the incoming traffic with IP-precedence values of 5, 6, and 7:

```
Device(config)# class-map class3
Device(config-cmap)# match ip precedence 5 6 7
Device(config-cmap)# exit
```

This example shows how to delete the IP-precedence match criteria and to classify traffic using acl1:

```
Device(config)# class-map class2
Device(config-cmap)# match ip precedence 5 6 7
Device(config-cmap)# no match ip precedence
Device(config-cmap)# match access-group acl1
Device(config-cmap)# exit
```

This example shows how to specify a list of physical ports to which an interface-level class map in a hierarchical policy map applies:

```
Device(config)# class-map match-any class4
Device(config-cmap)# match cos 4
Device(config-cmap)# exit
```

This example shows how to specify a range of physical ports to which an interface-level class map in a hierarchical policy map applies:

```
Device(config)# class-map match-any class4
Device(config-cmap)# match cos 4
Device(config-cmap)# exit
```

You can verify your settings by entering the **show class-map** privileged EXEC command.

match wlan user-priority

To match 802.11 specific values, use the **match wlan user-priority** command in class-map configuration mode. Use the **no** form of this command to return to the default setting.

match wlan user-priority *wlan-value* [*wlan-value*] [*wlan-value*] [*wlan-value*]
no match wlan user-priority *wlan-value* [*wlan-value*] [*wlan-value*] [*wlan-value*]

Syntax Description

wlan-value	The 802.11-specific values. Enter the user priority 802.11 TID user priority (0-7). (Optional) Enter up to three user priority values separated by white-spaces.

Command Default

None

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1 Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

None

This example show how you can configure user-priority values:

```
Device(config)# class-map test_1000
Device(config-cmap)# match wlan user-priority 7
```

max-bandwidth

To configure the wireless media-stream's maximum expected stream bandwidth in Kbps, use the **max-bandwidth** command.

max-bandwidth *bandwidth*

Syntax Description

bandwidth	Maximum Expected Stream Bandwidth in Kbps. Valid range is 1 to 35000 Kbps.

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 bandwidth in Kbps:

```
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)# max-bandwidth 3500
```

max-through

To limit multicast router advertisements (RAs) per VLAN per throttle period, use the **max-through** command in IPv6 RA throttle policy configuration mode. To reset the command to its defaults, use the **no** form of this command.

max-through {*mt-value* | **inherit** | **no-limit**}

Syntax Description

mt-value	Number of multicast RAs allowed on the VLAN before throttling occurs. The range is from 0 through 256.
inherit	Merges the setting between target policies.
no-limit	Multicast RAs are not limited on the VLAN.

Command Default

10 RAs per VLAN per 10 minutes

Command Modes

IPv6 RA throttle policy configuration (config-nd-ra-throttle)

Command History

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

Usage Guidelines

The **max-through** command limits the amount of multicast RAs that are passed through to the VLAN per throttle period. This command can be configured only on a VLAN.

Example

```
Device(config)# ipv6 nd ra-throttle policy policy1
Device(config-nd-ra-throttle)# max-through 25
```

mdns-sd

To configure the mDNS service discovery gateway, use the **mdns-sd** command. To disable the configuration, use the **no** form of this command.

mdns-sd { **gateway** | **service-definition** *service-definition-name* | **service-list** *service-list-name* { **IN** | **OUT** } | **service-policy** *service-policy-name* }

no mdns-sd { **gateway** | **service-definition** *service-definition-name* | **service-list** *service-list-name* { **IN** | **OUT** } | **service-policy** *service-policy-name* }

Syntax Description

mdns-sd	Configures the mDNS service discovery gateway.
gateway	Configures mDNS gateway.
service-definition	Configures mDNS service definition.
service-definition-name	Specifies the mDNS service definition name.
service-list	Configures mDNS service list.
service-list-name	Specifies the mDNS service definition name.
IN	Specifies the inbound filtering.
OUT	Specifies the outbound filtering.
service-policy	Configures mDNS service policy.
service-policy-name	Specifies the mDNS service policy name.

Command Default

None

Command Modes

Global configuration

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 mDNS service discovery gateway:

```
Device(config)# mdns-sd gateway
```

mdns-sd flex-profile

To configure the mDNS service discovery flex profile, use the **mdns-sd flex-profile** command. To disable the command, use the **no** form of this command.

mdns-sd flex-profile *flex-profile-name*

no mdns-sd flex-profile *flex-profile-name*

Syntax Description

mdns-sd flex-profile	Configures the mDNS service discovery flex profile.
flex-profile-name	Specifies the mDNS flex profile name.

Command Default

None

Command Modes

Global configuration

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 mDNS service discovery flex profile:

```
Device(config)# mdns-sd flex-profile mdns-flex-profile
```

mdns-sd profile

To apply the mDNS flex profile to the wireless flex profile, use the **mdns-sd profile** command in the wireless flex profile mode. To disable the command, use the **no** form of this command.

mdns-sd profile *flex-profile-name*

no mdns-sd profile *flex-profile-name*

Syntax Description

mdns-sd profile	Configures the mDNS flex profile in the wireless flex profile.
flex-profile-name	Specifies the mDNS flex profile name.

Command Default

None

Command Modes

Wireless flex profile configuration

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 apply the mDNS flex profile to the wireless flex profile:

```
Device(config-wireless-flex-profile)# mdns-sd profile mdns-flex-profile
```

method

To configure the primary and secondary supported Online Sign-Up (OSU) method of an OSU operator, use the **method** command. To to remove the OSU method, use the **no** form of the command.

method {**oma-dm** | **soap-xml-sp**}

Syntax Description

oma-dm	Sets OMA-DM as the primary or secondary OSU method for an OSU operator.
soap-xml-sp	Sets SOAP or XML-SPP as the primary or secondary OSU method for an OSU operator.

Command Default

None

Command Modes

ANQP OSU Provider Configuration (config-anqp-osu-provider)

Command History

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

Example

The following example shows how to configure the primary and secondary supported OSU method of the OSU operator:

```
Device(config-wireless-anqp-server)# osu-provider my-osu
Device(config-anqp-osu-provider)# method soap-xml-spp oma-dm
```

method fast

To configure EAP profile to support EAP-FAST method, use the **method fast** command.

method fast [**profile** *profile-name*]

Syntax Description

profile-name	Specify the method profile.

Command Default

None

Command Modes

config-eap-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 enable EAP Fast method on a EAP profile:

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

mgmtuser username

To set a username and password for AP management, use the **mgmtuser username** command. To disable this feature, use the **no** form of this command.

mgmtuser username *username* **password {0 | 8}** *password*

Syntax Description

username	Enter a username for AP management.
0	Specifies an UNENCRYPTED password.
8	Specifies an AES encrypted password.
password	Configures the encryption password (key).

Command Default

None

Command Modes

AP Profile Configuration (config-ap-profile)

Command History

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

Examples

The following example shows how to set a username and password for AP management:

```
Device# enable
Device# configure terminal
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# mgmtuser username myusername password 0
Device(config-ap-profile)# end
```

mobility backhaul-check coordinator-down

To configure URWB mobility backhaul-check when coordinator is unreachable, use the **mobility backhaul-check coordinator-down** {**handoff-inhibition** | **relay-switch**} command. Use the **no** form of this command to disable URWB mobility backhaul-check with coordinator-down

mobility backhaul-check coordinator-down { **handoff-inhibition** | **relay-switch** }

no mobility backhaul-check coordinator-down { **handoff-inhibition** | **relay-switch** }

Syntax Description

handoff-inhibition	Inhibits handoff if the coordinator is unreachable.
relay-switch	Switches to Infrastructure Wireless Relay mode if the coordinator is unreachable.

Command Default

None

Command Modes

Wireless URWB profile configuration (config-wireless-urwb-profile)

Command History

Release	Modification
Cisco IOS XE 17.18.1	This command was introduced.

Examples

The following example shows how to configure URWB mobility backhaul-check when coordinator is unreachable:

```
Device# configure terminal
Device(config)# wireless profile urwb urwb-profile-name
Device(config-wireless-urwb-profile)# mobility backhaul-check coordinator-down
handoff-inhibition
```

mobility backhaul-check eth-down

To configure URWB mobility backhaul-check when all Ethernet ports are disconnected, use the **mobility backhaul-check eth-down** {**handoff-inhibition** | **relay-switch**} command. Use the **no** form of this command to disable URWB mobility backhaul-check with the Ethernet ports disconnected.

mobility backhaul-check eth-down { **handoff-inhibition** | **relay-switch** }

no mobility backhaul-check eth-down { **handoff-inhibition** | **relay-switch** }

Syntax Description

handoff-inhibition	Inhibits handoff if all the Ethernet ports are down.
relay-switch	Switches to Infrastructure Wireless Relay mode if all the Ethernet ports are down.

Command Default

None

Command Modes

Wireless URWB profile configuration (config-wireless-urwb-profile)

Command History

Release	Modification
Cisco IOS XE 17.18.1	This command was introduced.

Examples

The following example shows how configure URWB mobility backhaul-check when all Ethernet ports are disconnected:

```
Device# configure terminal
Device(config)# wireless profile urwb urwb-profile-name
Device(config-wireless-urwb-profile)# mobility backhaul-check eth-down handoff-inhibition
```

mobility mpo cos

To configure the class-of-service (COS) packets to be protected through MPO, use the **mobility mpo cos** *cos-value* command.

mobility mpo cos *cos-value*

Syntax Description

cos-value	Specifies the COS value.

Command Default

The default value is 6.

Command Modes

Wireless URWB profile configuration (config-wireless-urwb-profile)

Command History

Release	Modification
Cisco IOS XE 17.18.1	This command was introduced.

Examples

The following example shows how to configure the class-of-service (COS) packets to be protected through MPO:

```
Device# configure terminal
Device(config)# wireless profile urwb urwb-profile-name
Device(config-wireless-urwb-profile)# mobility mpo cos 5
```

mobility mpo enable

To enable multipath operation (MPO) on RX and TX traffic, use the **mobility mpo enable** {**rx-only** | **tx-rx**}

mobility mpo enable { **rx-only** | **tx-rx** }

Syntax Description

rx-only	Enables the MPO feature only on the received traffic.
tx-rx	Enables the MPO feature bidirectionally.

Command Default

None

Command Modes

Wireless URWB profile configuration (config-wireless-urwb-profile)

Command History

Release	Modification
Cisco IOS XE 17.18.1	This command was introduced.

Examples

The following example shows how to configure URWB mobility backhaul-check when all Ethernet ports are disconnected:

```
Device# configure terminal
Device(config)# wireless profile urwb urwb-profile-name
Device(config-wireless-urwb-profile)# mobility mpo enable rx-only
```

mobility mpo path

To configure the maximum number of links on the backhaul radio, use the **mobility mpo path** *number-of-links* command.

mobility mpo path *number-of-links*

Syntax Description

number-of-links	Specifies the maximum number of links that need to be established for traffic duplication.

Command Default

The default value is 1.

Command Modes

Wireless URWB profile configuration (config-wireless-urwb-profile)

Command History

Release	Modification
Cisco IOS XE 17.18.1	This command was introduced.

Examples

The following example shows how configure the maximum number of links on the backhaul radio:

```
Device# configure terminal
Device(config)# wireless profile urwb urwb-profile-name
Device(config-wireless-urwb-profile)# mobility mpo path 1
```

mobility mpo rssi

To configure minimum RSSI to establish MPO redundant links, use the **mobility mpo rssi** *rssi-value*

mobility mpo rssi *rssi-value (0-96)*

Syntax Description

rssi-value	Specifies the RSSI value. The range is from 0 to 96.

Command Default

The default value is 0.

Command Modes

Wireless URWB profile configuration (config-wireless-urwb-profile)

Command History

Release	Modification
Cisco IOS XE 17.18.1	This command was introduced.

Examples

The following example shows how to configure minimum RSSI to establish MPO redundant links:

```
Device# configure terminal
Device(config)# wireless profile urwb urwb-profile-name
Device(config-wireless-urwb-profile)# mobility mpo rssi 0
```

mobility mpo telemetry

To configure multipath operation telemety, use the **mobility mpo telemetry** command.

mobility mpo telemetry

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Wireless URWB profile configuration (config-wireless-urwb-profile)

Command History

Release	Modification
Cisco IOS XE 17.18.1	This command was introduced.

Examples

The following example shows how to configure the class-of-service (COS) packets to be protected through MPO:

```
Device# configure terminal
Device(config)# wireless profile urwb urwb-profile-name
Device(config-wireless-urwb-profile)# mobility mpo telemetry
```

mobility role

To configure URWB mobility role, use the **mobility role**{ **base** | **base-relay** | **client**}

mobility role { **base** | **base-relay** | **client** }

Syntax Description

base	Specifies the mobility role base.
base-relay	Specifies the mobility role base relay.
client	Specifies the mobility role client.

Command Default

None

Command Modes

Wireless URWB profile configuration (config-wireless-urwb-profile)

Command History

Release	Modification
Cisco IOS XE 17.18.1	This command was introduced.

Examples

The following example shows how to configure the URWB mobility role:

```
Device# configure terminal
Device(config)# wireless profile urwb urwb-profile-name
Device(config-wireless-urwb-profile)# mobility role base
```

mobility scan

To configure mobility frequency scan feature, use the **mobility scan**{**isolation** *0-65535* | **periodic** *0-65535* | **rssi-threshold** *0-96*} command.

mobility scan { **isolation** *0-65535* | **periodic** *0-65535* | **rssi-threshold** *0-96* }

no mobility scan isolation

no mobility scan periodic

no mobility scan rssi-threshold

Syntax Description

isolation	Specifies that scanning takes place when the device is disconnected from the infrastructure.
periodic	Specifies a periodic background scanning.
rssi-threshold	Specifies that scanning takes place when RSSI falls below threshold.
0-65535	Specifies the maximum waiting-time after which the scanning is triggered (ms), for isolation and periodic scanning.
0-96	Specifies the threshold value.

Command Default

None

Command Modes

Wireless URWB profile configuration (config-wireless-urwb-profile)

Command History

Release	Modification
Cisco IOS XE 17.18.1	This command was introduced.

Examples

The following example shows how to configure mobility frequency scan feature:

```
Device# configure terminal
Device(config)# wireless profile urwb urwb-profile-name
Device(config-wireless-urwb-profile)# mobility scan isolation 3600
```

monitor capture (access list/class map)

To configure a monitor capture specifying an access list or a class map as the core filter for the packet capture, use the **monitor capture** command in privileged EXEC mode. To disable the monitor capture with the specified access list or class map as the core filter, use the **no** form of this command.

monitor capture *capture-name* { **access-list** *access-list-name* | **class-map** *class-map-name* }
no monitor capture *capture-name* { **access-list** *access-list-name* | **class-map** *class-map-name* }

Syntax Description

capture-name	The name of the capture.
access-list *access-list-name*	Configures an access list with the specified name.
class-map *class-map-name*	Configures a class map with the specified name.

Command Default

A monitor capture with the specified access list or a class map as the core filter for the packet capture is not configured.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced.

Usage Guidelines

Configure the access list using the **ip access-list** command or the class map using the **class-map** command before using the **monitor capture** command. You can specify a class map, or an access list, or an explicit inline filter as the core filter. If you have already specified the filter when you entered the **monitor capture match** command, the command replaces the existing filter.

Examples

The following example shows how to define a core system filter using an existing access control list:

```
Device> enable
Device# configure terminal
Device(config)# ip access-list standard acl1
Device(config-std-nacl)# permit any
Device(config-std-nacl)# exit
Device(config)# exit
Device# monitor capture mycap access-list acl1
Device# end
```

The following example shows how to define a core system filter using an existing class map:

```
Device> enable
Device# configure terminal
Device(config)# ip access-list standard acl1
Device(config-std-nacl)# permit any
Device(config-std-nacl)# exit
Device(config)# class-map match-all cmap
Device(config-cmap)# match access-group name acl
Device(config-cmap)# exit
```

```
Device(config)# exit
Device# monitor capture mycap class-map classmap1
Device# end
```

monitor capture export

To store captured packets in a file, use the **monitor capture export** command in privileged EXEC mode.

monitor capture *capture-name* **export** *filelocation* / *file-name*

Syntax Description

capture-name	Name of the capture.
export	Stores all the packets in capture buffer to a file of type .PCAP.
file-location/*file-name*	Destination file location and name.

Command Default

The captured packets are not stored.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Use the **monitor capture export** command only when the storage destination is a capture buffer. The file may be stored either remotely or locally. Use this command either during capture or after the packet capture has stopped. The packet capture could have stopped because one or more end conditions has been met or you entered the **monitor capture stop** command.

Examples

The following example shows how to export capture buffer contents:

```
Device> enable
Device# monitor capture mycap export tftp://10.1.88.9/mycap.pcap
Device# end
```

monitor capture (interface/control plane)

To configure monitor capture specifying an attachment point and the packet flow direction, use the **monitor capture** command in privileged EXEC mode. To disable the monitor capture with the specified attachment point and the packet flow direction, use the **no** form of this command.

monitor capture *capture-name* { **interface** *type number* | **control-plane** } { **in** | **out** | **both** }
no monitor capture *capture-name* { **interface** *type number* | **control-plane** } { **in** | **out** | **both** }

Syntax Description

capture-name	Name of the capture.
interface *type number*	Configures an interface with the specified type and number as an attachment point.
control-plane	Configures a control plane as an attachment point.
in	Specifies the inbound traffic direction.
out	Specifies the outbound traffic direction.
both	Specifies both inbound and outbound traffic directions.

Command Default

The monitor packet capture filter specifying is not configured.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Repeat the **monitor capture** command as many times as required to add multiple attachment points.

Examples

The following example shows how to add an attachment point to an interface:

```
Device> enable
Device# monitor capture mycap interface GigabitEthernet 0/0/1 in
Device# end
```

The following example shows how to add an attachment point to a control plane:

```
Device> enable
Device# monitor capture mycap control-plane out
Device# end
```

monitor capture limit

To configure capture limits, use the **monitor capture limit** command in privileged EXEC mode. To remove the capture limits, use the **no** form of this command.

monitor capture *capture-name* **limit** [**duration** *seconds*] [**every** *number*] [**packet-length** *size*] [**packets** *number*] [**pps** *number*]
no monitor capture *name* **limit** [**duration**] [**every**] [**packet-length**] [**packets**] [**pps**]

Syntax Description

capture-name	Name of the packet capture.
duration *seconds*	(Optional) Specifies the duration of the capture, in seconds. The range is from 1 to 1000000.
every *number*	(Optional) Specifies that, in a series of packets, the packet whose numerical order is denoted by the *number* argument should be captured. The range is from 2 to 100000.
packet-length *bytes*	(Optional) Specifies the packet length, in bytes. If the actual packet is longer than the specified length, only the first set of bytes whose number is denoted by the *bytes* argument is stored.
packets *packets-number*	(Optional) Specifies the number of packets to be processed for capture.
pps *pps-number*	(Optional) Specifies the number of packets to be captured per second. The range is from 1 to 1000000.

Command Default

No capture limits are configured.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

If no duration is specified, the capture does not stop until it is manually interrupted. The entire packet is processed if the **packet-length** *bytes* keyword-argument pair is not specified. All matched packets are captured, if the **every** *number* keyword-argument pair is not specified. All matched packets are captured if the **packets** *packets-number* keyword-argument pair is not specified. The incoming packets are captured at the rate of 1 million packets per second if the **pps** *number* keyword-argument pair is not specified.

Examples

The following example shows how to specify capture limits:

```
Device> enable
Device# monitor capture mycap limit duration 10
Device# monitor capture mycap limit packet-length 128
Device# monitor capture mycap limit packets 100
Device# monitor capture mycap limit pps 1000
```

```
Device# monitor capture mycap limit duration 10 packet-length 128 packets 100
Device# end
```

monitor capture match

To define an explicit inline core filter, use the **monitor capture match** command in privileged EXEC mode. To remove this filter, use the **no** form of this command.

monitor capture *capture-name* **match**
{ **any** | { **ipv4** | **ipv6** } { *source-prefix/length* | **any** | **host** } *source-ip-address* { { *destination-prefix/length* | **any** | **host** } *destination-ip-address* } | **protocol** { **tcp** | **udp** } { { *source-prefix/length* | **any** | **host** } { { *destination-prefix/length* | **any** | **host** } | [[**eq** | **gt** | **lt** | **neg**] *port-number*] | **range** *start-port-number end-port-number* | [**eq** | **gt** | **lt** | **neg**] *port-number* | **range** *start-port-number end-port-number* } } | **mac** { *source-mac-address* | { **any** | **host** } *source-mac-address* } *source-mac-address-mask* { *destination-mac-address* | { **any** | **host** } *destination-mac-address* } *destination-mac-address-mask* }
no monitor capture *capture-name* **match**

Syntax Description

epc-capture-name	Name of the capture.
any	Specifies all packets.
ipv4	Specifies IPv4 packets.
ipv6	Specifies IPv6 packets.
source-prefix/length	The network prefix and length of the IPv4 or IPv6 source address.
any	Specifies network prefix of any source IPv4 or IPv6 address.
host	Specifies the source host.
source-ip-address	Source IPv4 or IPv6 address.
destination-prefix/length	Destination IPv4 or IPv6 address.
any	Specifies the network prefix and length of any IPv4 or IPv6 destination address.
host	Specifies the destination host.
destination-ip-address	Destination IPv4 or IPv6 address.
protocol	Specifies the protocol.
tcp	Specifies the TCP protocol.
udp	Specifies the UDP protocol.
eq	(Optional) Specifies that only packets with a port number that is equal to the port number associated with the IP address are matched.

gt	(Optional) Specifies that only packets with a port number that is greater than the port number associated with the IP address are matched.
lt	(Optional) Specifies that only packets with a port number that is lower than the port number associated with the IP address are matched.
neq	(Optional) Specifies that only packets with a port number that is not equal to the port number associated with the IP address are matched.
port-number	(Optional) The port number associated with the IP address. The range is from 0 to 65535.
range	(Optional) Specifies the range of port numbers.
start-port-number	(Optional) The start of the range of port numbers. The range is from 0 to 65535.
end-port-number	(Optional) The end of the range of port numbers. The range is from 0 to 65535.
mac	Specifies a Layer 2 packet.
source-mac-address	The source MAC address.
any	Specifies the network prefix of any source MAC address.
host	Specifies the MAC source host.
source-mac-address-mask	The source MAC address mask.
destination-mac-address	The destination MAC address.
any	Specifies the network prefix of any destination MAC address.
host	Specifies the MAC source host.
destination-mac-address-mask	The destination MAC address mask.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 17.12.1	This command was introduced.

Usage Guidelines

Use the **monitor capture** command to specify the core filter as a class map, access list, or explicit inline filter. Any filter has already specified before you enter the **monitor capture match** command is replaced.

Examples

The following example shows how to set various explicit filters:

```
Device> enable
Device# monitor capture mycap match any
Device# monitor capture mycap match mac any any
Device# monitor capture mycap match ipv4 any any
Device# monitor capture mycap match ipv4 protocol udp 198.51.100.0/24 eq 20001 any
Device# end
```

The following example shows how to set a filter for MAC addresses:

```
Device> enable
Device# monitor capture match mycap mac 0030.9629.9f84 0000.0000.0000 0030.7524.9f84
0000.0000.0000
Device# end
```

The following example shows how to set a filter for IPv4 traffic:

```
Device> enable
Device# monitor capture match mycap ipv4 198.51.100.0/24 198.51.100.1 203.0.113.0/24
203.0.113.254
Device# end
```

monitor capture start

To start the capture of packet data at a traffic trace point into a buffer, use the **monitor capture start** command in privileged EXEC mode.

monitor capture *epc-capture-name* **start**

Syntax Description

epc-capture-name	Name of the capture.

Command Default

Data packets are not captured into a buffer.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Use the **monitor capture start** command to enable the packet data capture after the capture point is defined. To stop the capture of packet data, use the **monitor capture stop** command.

Ensure that system resources such as CPU and memory are available before starting a capture.

Examples

The following example shows how to start capture buffer contents:

```
Device> enable
Device# monitor capture mycap start
Device# monitor capture mycap export tftp://10.1.88.9/mycap.pcap
Device# monitor capture mycap limit packets 100 duration 60
Device# monitor capture mycap start
Device# end
```

monitor capture stop

To stop the capture of packet data at a traffic trace point, use the **monitor capture stop** command in privileged EXEC mode.

monitor capture *epc-capture-name* **stop**

Syntax Description

epc-capture-name	Name of the capture.

Command Default

The packet data capture is ongoing.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Use the **monitor capture start** command to start the capture of packet data that you started by using the **monitor capture start** command. You can configure two types of capture buffers: linear and circular. When the linear buffer is full, data capture stops automatically. When the circular buffer is full, data capture starts from the beginning and the data is overwritten.

Examples

The following example shows how to stop capture buffer contents:

```
Device> enable
Device# monitor capture mycap stop
Device# end
```

mop sysid

To enable an interface to send out periodic Maintenance Operation Protocol (MOP) system identification messages, use the **mopsysid** command in interface configuration mode. To disable MOP message support on an interface, use the **no** form of this command.

mop sysid
no mop sysid

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	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.

Usage Guidelines

You can still run MOP without having the background system ID messages sent. This command lets you use the MOP remote console, but does not generate messages used by the configurator.

Examples

The following example enables serial interface 0 to send MOP system identification messages:

```
Router(config)# interface serial 0
Router(config-if)# mop sysid
```

Related Commands

Command	Description
mop device-code	Identifies the type of device sending MOP sysid messages and request program messages.
mop enabled	Enables an interface to support the MOP.

mpls ether-filter ethernet-I

To configure URWB ether-filter Ethernet-I frames forwarding, use the **mpls ether-filter ethernet-I** command.

mpls ether-filter ethernet-I

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Wireless URWB profile configuration (config-wireless-urwb-profile)

Command History

Release	Modification
Cisco IOS XE 17.18.1	This command was introduced.

Examples

The following example shows how to configure URWB ether-filter Ethernet-I frames forwarding:

```
Device# configure terminal
Device(config)# wireless profile urwb urwb-profile-name
Device(config-wireless-urwb-profile)# mpls ether-filter ethernet-I
```

mpls ether-filter ethertypes filtering

To configure Ethernet type (L2 transparency) filtering method, use the **mpls ether-filter ethertypes filtering** {**allow-all** | **use-allow-list**}. Use the no form of this command to disable the feature.

mpls ether-filter ethertypes filtering { **allow-all** | **use-allow-list** }

no mpls ether-filter ethertypes filtering { **allow-all** | **use-allow-list** }

Syntax Description

allow-all	Specifies that the Ethernet type allows all ethertypes filtering.
use-allow-list	Specifies that only configured ethertypes allow-list is used.

Command Default

None

Command Modes

Wireless URWB profile configuration (config-wireless-urwb-profile)

Command History

Release	Modification
Cisco IOS XE 17.18.1	This command was introduced.

Examples

The following example shows how to configure Ethernet type (L2 transparency) filtering method:

```
Device# configure terminal
Device(config)# wireless profile urwb urwb-profile-name
Device(config-wireless-urwb-profile)# mpls ether-filter ethertypes filtering use-allow-list
```

mpls high-availability timeout

To configure the Multiprotocol Label Switching (MPLS) high availability node failure detection timeout, use the **mpls high-availability timeout** *timeout-value*. Use

mpls high-availability timeout *timeout-value*

no mpls high-availability

Syntax Description

timeout	Specifies the high availability node failure detection timeout, in seconds. The range is from 0 to 65535 seconds.

Command Default

None

Command Modes

Wireless URWB profile configuration (config-wireless-urwb-profile)

Command History

Release	Modification
Cisco IOS XE 17.18.1	This command was introduced.

Examples

The following example shows how to configure the Multiprotocol Label Switching (MPLS) high availability node failure detection timeout:

```
Device# configure terminal
Device(config)# wireless profile urwb urwb-profile-name
Device(config-wireless-urwb-profile)# mpls high-availability timeout 180
```

multicast (URWB)

To configure the multicast settings for the URWB profile, use the **multicast** {**all** | **coordinator-only**} command. Use the **no** form of the command to disable the URWB multicast settings.

multicast { **all** | **coordinator-only** }

no multicast

Syntax Description

all	Enables the multicast rule as a broadcast.
coordinator-only	Enables the multicast rule to the coordinator only.

Command Default

None

Command Modes

Wireless URWB profile configuration (config-wireless-urwb-profile)

Command History

Release	Modification
Cisco IOS XE 17.18.1	This command was introduced.

Examples

The following example shows how to configure the multicast settings for the URWB profile:

```
Device# configure terminal
Device(config)# wireless profile urwb urwb-profile-name
Device(config-wireless-urwb-profile)# multicast coordinator-only
```

multicast vlan

To configure multicast on a single VLAN, use the **multicast vlan** command. To remove the multicast, use the **no** form of the command.

multicast vlan *vlan-id*
no multicast vlan *vlan-id*

Syntax Description

vlan-id	Specifies the VLAN ID.

Command Default

Disabled.

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 multicast:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy policy-test
Device(config-wireless-policy)# multicast vlan 12
```

name

To configure the name of the Online Sign-Up (OSU) operator in a given language, use the **name** command. To remove the name of the OSU operator, use the **no** form of the command.

name *operator-name language-code* [*service-description*]

Syntax Description

operator-name	OSU operator name.
language-code	A three character language code for the operator. Use only the first three letters of the language, in lower case, for the language code. For example, use *eng* for English. To see the full list of language codes, go to: http://www.loc.gov/standards/iso639-2/php/code_list.php.
service-description	Service description for the OSU operator.

Command Default

None

Command Modes

ANQP OSU Provider Configuration (config-anqp-osu-provider)

Command History

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

Example

The following example shows how to configure the name of an OSU operator in a given language:

```
Device(config-wireless-anqp-server)# osu-provider my-osu
Device(config-anqp-osu-provider)# name xxy eng
```

nac

To enable RADIUS Network Admission Control (NAC) support, use the **nac** command. To disable NAC support, use the **no** form of this command.

nac [**ise** | **xwf**]
no nac

Syntax Description

ise	Configures Radius NAC support (Identity Service Engine)
xwf	Configures Express Wi-Fi NAC support.

Command Default

NAC is disabled.

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 RADIUS NAC:

```
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)# nac
```

nai-realm

To configure the 802.11u Network Access Identifier (NAI) realm, use the **nai-realm** command. To remove the realm, use the **no** form of the command.

nai-realm *nai-realm*

Syntax Description

nai-realm	NAI realm name. The realm 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 the 802.11u NAI realm:

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# nai-realm cisco.com
```

nai-realm (OSU Provider)

To configure the Network Access Identifier (NAI) realm of the OSU operator, use the **nai-realm** command. To remove the realm of the OSU operator, use the **no** form of the command.

nai-realm *nai-realm*

Syntax Description

nai-realm	NAI realm name. The realm name should not exceed 220 characters.

Command Default

None

Command Modes

ANQP OSU Provider Configuration (config-anqp-osu-provider)

Command History

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

Example

The following example shows how to configure the NAI realm of the OSU operator:

```
Device(config-anqp-osu-provider)# nai-realm cisco.com
```

nas-id option2

To configure option 2 parameters for a NAS-ID, use the **nas-id option2** command.

nas-id option2 {**sys-ip** | **sys-name** | **sys-mac** }

Syntax Description

sys-ip	System IP Address.
sys-name	System Name.
sys-mac	System MAC address.

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 configure the system IP address for the NAS-ID:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless aaa policy profile-name
Device(config-aaa-policy)# nas-id option2 sys-ip
```

network

To configure the network number in decimal notation, use the **network** command.

network *network-number* [*network-mask* | **secondary**]

Syntax Description

ipv4-address	Network number in dotted-decimal notation.
network-mask	Network mask or prefix length.
secondary	Configure as secondary subnet.

Command Default

None

Command Modes

dhcp-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 network number and the mask address:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ip dhcp pool name
Device(dhcp-config)# network 209.165.200.224 255.255.255.0
```

network-key key

To configure the shared network key, use the **network-key key** {**0** | **8**} *network-key*

network-key key { **0** | **8** } *network-key*

Syntax Description

0 | 8	Here, **0** specifies that an unencrypted network key will follow, and **8** specifies that an AES encrypted network-key will follow.
network-key	Specifies the shared key of the network.

Command Default

None

Command Modes

Wireless URWB profile configuration (config-wireless-urwb-profile)

Command History

Release	Modification
Cisco IOS XE 17.18.1	This command was introduced.

Usage Guidelines

The network key is shared with all the devices in the same URWB network.

Examples

The following example shows how to configure the shared network key:

```
Device# configure terminal
Device(config)# wireless profile urwb urwb-profile-name
Device(config-wireless-urwb-profile)# network-key key {0 | 8} network-key
```

network-type

To configure the 802.11u network type, use the **network-type** command. To remove the network type, use the **no** form of the command.

network-type { **chargeable-public** | **emergency** | **free-public** | **guest-private** | **personal-device** | **private** | **test** | **wildcard** } **internet-access** { **allowed** | **forbidden** }

Syntax Description

chargeable-public	Sets as chargeable public network.
emergency	Sets as emergency network.
free-public	Sets as free public network.
guest-private	Sets as guest private network.
personal-device	Sets as personal device network.
private	Sets as private network.
test	Sets as test network.
wildcard	Sets as wildcard network.
internet-access	Configures network ability to access the internet.
allowed	Enables internet access.
disabled	Disables internet access.

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 802.11u network type:

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# network-type wildcard internet-access allowed
```

nmsp cloud-services enable

To configure NMSP cloud services, use the **nmsp cloud-services enable** command.

nmsp cloud-services enable

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 NMSP cloud services:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# nmsp cloud-services enable
```

nmsp cloud-services http-proxy

To configure the proxy for NMSP cloud server, use the **nmsp cloud-services http-proxy** command.

nmsp cloud-services http-proxy *proxy-server port*

Syntax Description

proxy-server	Enter the hostname or the IP address of the proxy server for NMSP cloud services.
port	Enter the proxy server port number for NMSP cloud services.

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 proxy for NMSP cloud server:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# nmsp cloud-services http-proxy host-name port-number
```

nmsp cloud-services server token

To configure the NMSP cloud services server parameters, use the **nmsp cloud-services server token** command.

nmsp cloud-services server token *token*

Syntax Description

token	Authentication token for the NMSP cloud services.

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 the for the NMSP cloud services server parameters:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# nmsp cloud-services server token authentication-token
```

nmsp cloud-services server url

To configure NMSP cloud services server URL, use the **nmsp cloud-services server url** command.

nmsp cloud-services server url *url*

Syntax Description

url	URL of the NMSP cloud services server.

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 a URL for NMSP cloud services server:

```
Device(config)# nmps cloud-services server url http://www.example.com
```

nmsp notification interval

To modify the Network Mobility Services Protocol (NMSP) notification interval value on the controller to address latency in the network, use the **nmsp notification interval** command in global configuration mode.

nmsp notification interval { **attachment** | **location** | **rssi** {**clients** | **rfid** | **rogues** {**ap** | **client** } } }

Syntax Description

attachment	Specifies the time used to aggregate attachment information.
location	Specifies the time used to aggregate location information.
rssi	Specifies the time used to aggregate RSSI information.
clients	Specifies the time interval for clients.
rfid	Specifies the time interval for rfid tags.
rogues	Specifies the time interval for rogue APs and rogue clients .
ap	Specifies the time used to aggregate rogue APs .
client	Specifies the time used to aggregate rogue clients.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1 Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

This example shows how to set the NMSP notification interval for the active RFID tags to 25 seconds:

```
Device# configure terminal
Device(config)# nmsp notification-interval rfid 25
Device(config)# end
```

This example shows how to modify NMSP notification intervals for device attachment (connecting to the network or disconnecting from the network) every 10 seconds:

```
Device# configure terminal
Device(config)# nmsp notification-interval attachment 10
Device(config)# end
```

This example shows how to configure NMSP notification intervals for location parameters (location change) every 20 seconds:

```
Device# configure terminal
Device(config)# nmsp notification-interval location 20
Device(config)# end
```

nmsp strong-cipher

To enable the new ciphers, use the **nmsp strong-cipher** command in global configuration mode. To disable, use the **no** form of this command.

nmsp strong-cipher
no nmsp strong-cipher

Syntax Description

This command has no arguments or keywords.

Command Default

The new ciphers are not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(2)E	This command was introduced.

Usage Guidelines

The **nmsp strong-cipher** command enables strong ciphers for new Network Mobility Service Protocol (NMSP) connections.

Note The existing NMSP connections will use the default cipher.

Examples

The following example shows how to enable a strong-cipher for NMSP:

```
Device> enable
Device> configure terminal
Device(config)# nmsp strong-cipher
```

Related Commands

Command	Description
show nmsp status	Displays the status of active NMSP connections.

no shutdown (URWB)

To enable the URWB profile, use the **no shutdown** command in the wireless URWB profile configuration mode.

no shutdown

Syntax Description

This command has no keywords or arguments.

Command Modes

Wireless URWB profile configuration (config-wireless-urwb-profile)

Command History

Release	Modification
Cisco IOS XE 17.18.1	This command was introduced.

Examples

The following example shows how to enable the URWB profile:

```
Device# configure terminal
Device(config)# wireless profile urwb urwb-profile-name
Device(config-wireless-urwb-profile)# no shutdown
```

operator

To configure a Hotspot 2.0 operator-friendly name in a given language, use the **operator** command. To remove the operator name, use the **no** form of the command.

operator *operator-name language-code*

Syntax Description

operator-name	Name of the operator.
language-code	A three character language code for the operator. Use only the first three letters of the language, in lower case, for the language code. For example, use *eng* for English. To see the full list of language codes, go to: http://www.loc.gov/standards/iso639-2/php/code_list.php.

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 an operator-friendly name:

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# operator XYZ-operator eng
```

operating-class

To configure a Hotspot 2.0 operating class identifier, use the **operating-class** command. To remove the operating class, use the **no** form of the command.

operating-class *class-id*

Syntax Description

class-id	Operating class ID number.

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 an operating class identifier:

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# operating-class 25
```

option

To configure optional data parameters for a flow exporter for , use the **option** command in flow exporter configuration mode. To remove optional data parameters for a flow exporter, use the **no** form of this command.

option {**exporter-stats** | **interface-table** | **sampler-table**} [**timeout** *seconds*]
no option {**exporter-stats** | **interface-table** | **sampler-table**}

Syntax Description

exporter-stats	Configures the exporter statistics option for flow exporters.
interface-table	Configures the interface table option for flow exporters.
sampler-table	Configures the export sampler table option for flow exporters.
timeout *seconds*	(Optional) Configures the option resend time in seconds for flow exporters. The range is 1 to 86400. The default is 600.

Command Default

The timeout is 600 seconds. All other optional data parameters are not configured.

Command Modes

Flow exporter configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1 Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

The **option exporter-stats** command causes the periodic sending of the exporter statistics, including the number of records, bytes, and packets sent. This command allows the collector to estimate packet loss for the export records it receives. The optional timeout alters the frequency at which the reports are sent.

The **option interface-table** command causes the periodic sending of an options table, which allows the collector to map the interface SNMP indexes provided in the flow records to interface names. The optional timeout can alter the frequency at which the reports are sent.

The **option sampler-table** command causes the periodic sending of an options table, which details the configuration of each sampler and allows the collector to map the sampler ID provided in any flow record to a configuration that it can use to scale up the flow statistics. The optional timeout can alter the frequency at which the reports are sent.

To return this command to its default settings, use the **no option** or **default option** flow exporter configuration command.

The following example shows how to enable the periodic sending of the sampler option table, which allows the collector to map the sampler ID to the sampler type and rate:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# option sampler-table
```

The following example shows how to enable the periodic sending of the exporter statistics, including the number of records, bytes, and packets sent:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# option exporter-stats
```

The following example shows how to enable the periodic sending of an options table, which allows the collector to map the interface SNMP indexes provided in the flow records to interface names:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# option interface-table
```

osu-provider

To configure a Hotspot 2.0 online sign up (OSU) provider, use the **osu-provider** command. Use the **no** form of the command to remove the OSU provider.

osu-provider *provider-name*

Syntax Description

provider-name	Name of the OSU provider.

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 an OSU provider:

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# osu-provider yyy
```

osu-ssid

To configure the service set Identifier (SSID) for the wireless client to use for online sign-up (OSU), use the **osu-ssid** command. To remove the SSID, use the **no** form of the command.

osu-ssid *ssid*

Syntax Description

ssid	Name of the SSID for the wireless client. The SSID length can be up to 32 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 the SSID for the wireless client to use during OSU:

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# osu-ssid cisco
```

parameter-map type subscriber attribute-to-service

To configure parameter map type and name, use the **parameter-map type subscriber attribute-to-service** command.

parameter-map type subscriber attribute-to-service *parameter-map-name*

Syntax Description

attribute-to-service	Name the attribute to service.
parameter-map-name	Name of the parameter map. The map name is limited to 33 characters.

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 parameter map type and name:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# parameter-map type subscriber attribute-to-service parameter-map-name
```

parameter-map type webauth

To configure the webauth parameter type for a specific parameter map or all the parameter maps, use the **parameter-map type webauth** command.

parameter-map type webauth { *parameter-map-name* | **global** }

Syntax Description

parameter-map-name	Name of the parameter map. The map name is limited to 99 characters.
global	Applies the configuration to all the parameter maps.

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 webauth parameter type for a parameter map named *parameter-map1*:

```
Device# configure terminal
Device(config)# parameter-map type webauth parameter-map1
```

password encryption aes

To enable strong (AES) password encryption, use the **password encryption aes** command. To disable this feature, use the **no** form of this command.

password encryption aes
`no password encryption aes`

Syntax Description

password	Configures the encryption password (key).
encryption	Encrypts system passwords.
aes	Enables stronger (AES) password encryption.

Command Default

None

Command Modes

Global configuration mode.

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

The following example shows how to enable AES password encryption :

```
Device(config)#password encryption aes
```

peer-blocking

To configure peer-to-peer blocking on a WLAN, use the **peer-blocking** command. To disable peer-to-peer blocking, use the **no** form of this command.

peer-blocking {**drop** | **forward-upstream**}
no peer-blocking

Syntax Description

drop	Specifies the device to discard the packets.
forward-upstream	Specifies the packets to be forwarded on the upstream VLAN. The device next in the hierarchy to the device decides what action to take regarding the packets. **Note** The **forward-upstream** option is not supported for Flex local switching. Traffic is dropped even if this option is configured. Also, peer to peer blocking for local switching SSIDs are available only for the clients on the same AP.

Command Default

Peer blocking is disabled.

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 enable the drop and forward-upstream options for peer-to-peer blocking:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1

Device(config-wlan)# peer-blocking  drop
Device(config-wlan)# peer-blocking forward-upstream
```

This example shows how to disable the drop and forward-upstream options for peer-to-peer blocking:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1

Device(config-wlan)# no peer-blocking  drop
Device(config-wlan)# no peer-blocking forward-upstream
```

policy

To configure media stream admission policy, use the **policy** command.

policy {**admit** | **deny**}

Syntax Description

admit	Allows traffic for a media stream group.
deny	Denies traffic for a media stream group.

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 allow traffic for a media stream group:

```
Device # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless media-stream group ms-group 224.0.0.0 224.0.0.223
Device(media-stream)# policy admit
```

police

To define a policer for classified traffic, use the **police** command in policy-map class configuration mode. Use the **no** form of this command to remove an existing policer.

police *rate-bps burst-byte* [**conform-action transmit**]
no police rate-bps *burst-byte* [**conform-action transmit**]

Syntax Description

rate-bps	Specify the average traffic rate in bits per second (b/s). The range is 1000000 to 1000000000.
burst-byte	Specify the normal burst size in bytes. The range is 8000 to 1000000.
conform-action transmit	(Optional) When less than the specified rate, specify that the switch transmits the packet.

Command Default

No policers are defined.

Command Modes

Policy-map class configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1 Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

A policer defines a maximum permissible rate of transmission, a maximum burst size for transmissions, and an action to take if either maximum is exceeded.

When configuring hierarchical policy maps, you can only use the **police** policy-map command in a secondary interface-level policy map.

The port ASIC device, which controls more than one physical port, supports 256 policers on the switch (255 user-configurable policers plus 1 policer reserved for internal use). The maximum number of configurable policers supported per port is 63. Policers are allocated on demand by the software and are constrained by the hardware and ASIC boundaries. You cannot reserve policers per port. There is no guarantee that a port will be assigned to any policer.

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

Examples

This example shows how to configure a policer that transmits packets if traffic is less than 1 Mb/s average rate with a burst size of 20 KB. There is no packet modification.

```
Device(config)# class-map class1
Device(config-cmap)# exit
Device(config)# policy-map policy1
Device(config-pmap)# class class1
Device(config-pmap-c)# police 1000000 20000 conform-action transmit
```

```
Device(config-pmap-c)# exit
```

This example shows how to configure a policer that transmits packets if traffic is less than 1 Mb/s average rate with a burst size of 20 KB. There is no packet modification. This example uses an abbreviated syntax:

```
Device(config)# class-map class1
Device(config-cmap)# exit
Device(config)# policy-map policy1
Device(config-pmap)# class class1
Device(config-pmap-c)# police 1m 20000 conform-action transmit
Device(config-pmap-c)# exit
```

This example shows how to configure a policer, which marks down the DSCP values with the values defined in policed-DSCP map and sends the packet:

```
Device(config)# policy-map policy2
Device(config-pmap)# class class2
Device(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
Device(config-pmap-c)# exit
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

police cir

To set the policing of committed information rate, use the **police cir** command.

police cir *<target bit rate>*

Syntax Description

police cir	Polices committed information rate.
8000-10000000000	Sets the target bit rate at bits per second. The range is between 8000 and 10000000000.

Command Default

None

Command Modes

Policy map class configuration

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.2.1	This command was introduced.

Example

This example shows how to set the committed information rate:

```
Device(config-pmap-c)#police cir 8000
```

policy-map

To create or modify a policy map that can be attached to multiple physical ports or switch virtual interfaces (SVIs) and to enter policy-map configuration mode, use the **policy-map** command in global configuration mode. Use the **no** form of this command to delete an existing policy map and to return to global configuration mode.

policy-map *policy-map-name*
no policy-map *policy-map-name*

Syntax Description

policy-map-name	Name of the policy map.

Command Default

No policy maps are defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1 Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

After entering the **policy-map** command, you enter policy-map configuration mode, and these configuration commands are available:

- **class**—Defines the classification match criteria for the specified class map.
- **description**—Describes the policy map (up to 200 characters).
- **exit**—Exits policy-map configuration mode and returns you to global configuration mode.
- **no**—Removes a previously defined policy map.
- **sequence-interval**—Enables sequence number capability.

To return to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

Before configuring policies for classes whose match criteria are defined in a class map, use the **policy-map** command to specify the name of the policy map to be created, added to, or modified. Entering the **policy-map** command also enables the policy-map configuration mode in which you can configure or modify the class policies for that policy map.

You can configure class policies in a policy map only if the classes have match criteria defined for them. To configure the match criteria for a class, use the **class-map** global configuration and **match** class-map configuration commands. You define packet classification on a physical-port basis.

Only one policy map per ingress port is supported. You can apply the same policy map to multiple physical ports.

You can apply a nonhierarchical policy maps to physical ports. A nonhierarchical policy map is the same as the port-based policy maps in the device.

A hierarchical policy map has two levels in the format of a parent-child policy. The parent policy cannot be modified but the child policy (port-child policy) can be modified to suit the QoS configuration.

In VLAN-based QoS, a service policy is applied to an SVI interface.

Note Not all MQC QoS combinations are supported for wired ports. For information about these restrictions, see chapters "Restrictions for QoS on Wired Targets" in the QoS configuration guide.

Examples

This example shows how to create a policy map called policy1. When attached to the ingress port, it matches all the incoming traffic defined in class1, sets the IP DSCP to 10, and polices the traffic at an average rate of 1 Mb/s and bursts at 20 KB. Traffic less than the profile is 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 transmit
Device(config-pmap-c)# exit
```

This example show you how to configure hierarchical polices:

```
Device# configure terminal
Device(config)# class-map c1
Device(config-cmap)# exit

Device(config)# class-map c2
Device(config-cmap)# exit

Device(config)# policy-map child
Device(config-pmap)# class c1
Device(config-pmap-c)# priority level 1
Device(config-pmap-c)# police rate percent 20 conform-action transmit exceed action drop
Device(config-pmap-c-police)# exit
Device(config-pmap-c)# exit

Device(config-pmap)# class c2
Device(config-pmap-c)# bandwidth 20000
Device(config-pmap-c)# exit

Device(config-pmap)# class class-default
Device(config-pmap-c)# bandwidth 20000
Device(config-pmap-c)# exit
Device(config-pmap)# exit

Device(config)# policy-map parent
Device(config-pmap)# class class-default
Device(config-pmap-c)# shape average 1000000
Device(config-pmap-c)# service-policy child
Deviceconfig-pmap-c)# end
```

This example shows how to delete a policy map:

```
Device(config)# no policy-map policymap2
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

policy-map

To create or modify a policy map that can be attached to multiple physical ports or switch virtual interfaces (SVIs) and to enter policy-map configuration mode, use the **policy-map** command in global configuration mode. Use the **no** form of this command to delete an existing policy map and to return to global configuration mode.

policy-map *policy-map-name*
no policy-map *policy-map-name*

Syntax Description

policy-map-name	Name of the policy map.

Command Default

No policy maps are defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1 Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

After entering the **policy-map** command, you enter policy-map configuration mode, and these configuration commands are available:

- **class**—Defines the classification match criteria for the specified class map.
- **description**—Describes the policy map (up to 200 characters).
- **exit**—Exits policy-map configuration mode and returns you to global configuration mode.
- **no**—Removes a previously defined policy map.
- **sequence-interval**—Enables sequence number capability.

To return to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

Before configuring policies for classes whose match criteria are defined in a class map, use the **policy-map** command to specify the name of the policy map to be created, added to, or modified. Entering the **policy-map** command also enables the policy-map configuration mode in which you can configure or modify the class policies for that policy map.

You can configure class policies in a policy map only if the classes have match criteria defined for them. To configure the match criteria for a class, use the **class-map** global configuration and **match** class-map configuration commands. You define packet classification on a physical-port basis.

Only one policy map per ingress port is supported. You can apply the same policy map to multiple physical ports.

You can apply a nonhierarchical policy maps to physical ports. A nonhierarchical policy map is the same as the port-based policy maps in the device.

A hierarchical policy map has two levels in the format of a parent-child policy. The parent policy cannot be modified but the child policy (port-child policy) can be modified to suit the QoS configuration.

In VLAN-based QoS, a service policy is applied to an SVI interface.

Note Not all MQC QoS combinations are supported for wired ports. For information about these restrictions, see chapters "Restrictions for QoS on Wired Targets" in the QoS configuration guide.

Examples

This example shows how to create a policy map called policy1. When attached to the ingress port, it matches all the incoming traffic defined in class1, sets the IP DSCP to 10, and polices the traffic at an average rate of 1 Mb/s and bursts at 20 KB. Traffic less than the profile is 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 transmit
Device(config-pmap-c)# exit
```

This example show you how to configure hierarchical polices:

```
Device# configure terminal
Device(config)# class-map c1
Device(config-cmap)# exit

Device(config)# class-map c2
Device(config-cmap)# exit

Device(config)# policy-map child
Device(config-pmap)# class c1
Device(config-pmap-c)# priority level 1
Device(config-pmap-c)# police rate percent 20 conform-action transmit exceed action drop
Device(config-pmap-c-police)# exit
Device(config-pmap-c)# exit

Device(config-pmap)# class c2
Device(config-pmap-c)# bandwidth 20000
Device(config-pmap-c)# exit

Device(config-pmap)# class class-default
Device(config-pmap-c)# bandwidth 20000
Device(config-pmap-c)# exit
Device(config-pmap)# exit

Device(config)# policy-map parent
Device(config-pmap)# class class-default
Device(config-pmap-c)# shape average 1000000
Device(config-pmap-c)# service-policy child
Deviceconfig-pmap-c)# end
```

This example shows how to delete a policy map:

```
Device(config)# no policy-map policymap2
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

port

To configure the port number to use when configuring the custom application, use the **port** command.

port *port-no*

Syntax Description

port-no	Port number.

Command Default

None

Command Modes

config-custom

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 port number to use when configuring the custom application:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ip nbar custom custom-protocol http host host-string
Device(config-custom)# http host hostname
Device(config-custom)# port port-no
```

priority priority-value

To configure media stream priority, use the **priority** *priority-value* command.

priority *priority-value*

Syntax Description

priority-value	Media stream priority value. Valid range is 1 to 8, with 1 being lowest priority and 8 being highest priority.

Command Default

None

Command Modes

config-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 set the media stream priority value to the highest, that is 8:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless media-stream group my-media-group 224.0.0.0 224.0.0.223
Device(config-media-stream)# priority 8
```

public-ip

To configure the NAT public IP address of the controller, use the **public-ip** command.

public-ip { *ipv4-address* | *ipv6-address* }

Syntax Description

ipv4-address	Sets IPv4 address.
ipv6-address	Sets IPv6 address.

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 the NAT public IP address of the controller:

```
Device# configure terminal
Device(config)# wireless management interface Vlan1
Device(config-mgmt-interface)# public-ip 192.168.172.100
```

qos-map

To configure a quality of service (QoS) map, use the **qos-map** command in ap profile configuration mode.

Use the **no** form of the command to disable the configuration.

qos-map { **action-frame** | **dscp-to-up-exception** *dscp-value user-priority* | **dscp-to-up-range** *user-priority dscp-value lower-dscp-range upper-dscp-range* | **trust-dscp-upstream** }

Syntax Description

action-frame	Sends the 802.11 QoS map action frame when the QoS map configuration is changed.
dscp-to-up-exception	Provides DSCP-to-user priority mapping exception.
dscp-to-up-range	Provides DSCP-to-user priority mapping. To delete all the custom mapping, use the **no dscp-to-up-range** command.
dscp-value	User priority-to-DSCP upstream. Valid range is from 0-63.
user-priority	User priority. Valid range is from 1-7.
lower-dscp-range	Lower-end of the DSCP range. Valid range is from 0-63.
upper-dscp-range	Upper-end of the DSCP range. Valid range is from 0-63.
trust-dscp-upstream	Instructs an access point (AP) to trust upstream DSCP instead of user priority.

Command Default

None

Command Modes

AP Profile Configuration (config-ap-profile)

Command History

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

Usage Guidelines

For internetworking with IP networks, a mapping is devised between the 802.11e user priorities and IP DSCP.

The mapping is specified as DSCP ranges to individual UP values, and as a set of exceptions with one-to-one mapping between DSCP values and UP values. If the QoS Map is enabled and user configurable mappings are not added, then the default values are used.

You can configure up to eight configuration entries for *user-priority*; one for each *user-priority* value. If you do not configure a custom value, a non-configured value (0xFF) is sent to the corresponding AP and the wireless clients.

For **dscp-to-up-exception**, you can configure a maximum of 21 entries.

The following table shows a QoS map where the corresponding AP provides a wireless client with the required mapping from IP DSCP to 802.11e user priorities.

Table 2: Default DSCP-range to UP Mapping

IP DSCP Range	802.11e User Priority
0-7	0
8-15	1
16-23	2
24-31	3
32-39	4
40-47	5
48-55	6
56-63	7

The following table shows the set of exceptions with one-to-one mapping between DSCP values and user priority values.

Table 3: Default DSCP-range to UP Mapping Exceptions

IP DSCP	802.11e User Priority
0	0
2	1
4	1
6	1
10	2
12	2
14	2
18	3
20	3
22	3
26	4
34	5
46	6
48	7
56	7

Example

The following example shows how to configure a QoS map:

```
Device(config)# ap profile hotspot
Device(config-ap-profile)# qos-map dscp-to-up-range 6 52 23 62
```

qos video

To configure over-the-air QoS class to video only, use the **qos video** command.

qos video

Command Default None

Command Modes config-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 over-the-air QoS class to video only:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless media-stream group my-media-group 224.0.0.0 224.0.0.223
Device(config-media-stream)# qos video
```

radius server

To configure the RADIUS server, use the **radius server** command in global configuration mode.

radius server *server-name*

Syntax Description

server-name	RADIUS server name.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1 Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

The length of the radius name is a variable. However, the parser restricts the CLI length of 256 characters including the **no** form of the command.

The following example shows how to configure a radius server:

```
Device(config)# radius server ISE
```

radius-server deadtime

To improve RADIUS response times when some servers might be unavailable, use the **radius-server deadtime** command to cause the unavailable servers to be skipped immediately. To set dead-time to the default value of 0, use the **no** form of this command.

radius-server deadtime *time-in-minutes*

no radius-server deadtime

Syntax Description

time-in-minutes	Length of time, in minutes, for which a RADIUS server is skipped over by transaction requests, up to a maximum of 1440 minutes (24 hours).

Command Default

Dead time is set to 0.

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

Use this command to mark as "dead" any RADIUS servers that fail to respond to authentication requests, thus avoiding the wait for the request to time out before trying the next configured server. A RADIUS server marked as "dead" is skipped by additional requests for the duration of minutes or unless there are no servers not marked "dead."

Example

The following example shows how to set deadtime for RADIUS servers that fail to respond to authentication requests:

```
Device(config)# radius-server deadtime 5
```

radius-server attribute wireless accounting call-station-id

To configure call station identifier sent in the RADIUS accounting messages, use the **radius-server attribute wireless accounting call-station-id** command. To remove the call station identifier from the radius accounting messages, use the **no** form of the command.

radius-server attribute wireless authentication call-station-id { **ap-ethmac-only** | **ap-ethmac-ssid** | **ap-ethmac-ssid-flexprofilename** | **ap-ethmac-ssid-policytagname** | **ap-ethmac-ssid-sitetagname** | **ap-group-name** | **ap-label-address** | **ap-label-address-ssid** | **ap-location** | **ap-macaddress** | **ap-macaddress-ssid** | **ap-macaddress-ssid-flexprofilename** | **ap-macaddress-ssid-policytagname** | **ap-macaddress-ssid-sitetagname** | **ap-name** | **ap-name-ssid** | **flex-profile-name** | **ipaddress** | **macaddress** | **policy-tag-name** | **site-tag-name** | **vlan-id** }

Syntax Description

ap-ethmac-only	Sets the call station identifier type to be AP's radio MAC address.
ap-ethmac-ssid	Sets the call station identifier type AP's radio MAC address with SSID.
ap-ethmac-ssid-flexprofilename	Sets the call station identifier type AP's radio MAC address with SSID and flex profile name.
ap-ethmac-ssid-policytagname	Sets the call station identifier type AP's radio MAC address with SSID and policy tag name.
ap-ethmac-ssid-sitetagname	Sets the call station identifier type AP's radio MAC address with SSID and site tag name.
ap-group-name	Sets the call station identifier type to use the AP group name.
ap-label-address	Sets the call station identifier type to the AP's radio MAC address that is printed on the AP label.
ap-label-address-ssid	Sets the call station identifier type to the AP's radio MAC address and SSID that is printed on the AP label.
ap-location	Sets the call station identifier type to the AP location.
ap-macaddress	Sets the call station identifier type to the AP's radio MAC address.
ap-macaddress-ssid	Sets the call station identifier type to the AP's radio MAC address with SSID.
ap-macaddress-ssid-flexprofilename	Sets the call station identifier type to the AP's radio MAC address with SSID and flex profile name.
ap-macaddress-ssid-policytagname	Sets the call station identifier type to the AP's radio MAC address with SSID and policy tag name.
ap-macaddress-ssid-sitetagname	Sets the call station identifier type to the AP's radio MAC address with SSID and site tag name.
ap-name	Sets the call station identifier type to the AP name.

ap-name-ssid	Sets the call station identifier type to the AP name with SSID.
flex-profile-name	Sets the call station identifier type to the flex profile name.
ipaddress	Sets the call station identifier type to the IP address of the system.
macaddress	Sets the call station identifier type to the MAC address of the system.
policy-tag-name	Sets the call station identifier type to the policy tag name.
site-tag-name	Sets the call station identifier type to the site tag name.
vlan-id	Sets the call station identifier type to the system's VLAN ID.

Command Default

Call station identifier is not configured.

Command Modes

Global Configuration(config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.
Cisco IOS XE Bengaluru 17.4.1	This command was modified. The **policy-tag-name**, **flex-profile-name**, **ap-macaddress-ssid-flexprofilename**, **ap-macaddress-ssid-policytagname**, **ap-macaddress-ssid-sitetagname**, **ap-ethmac-ssid-flexprofilename**, **ap-ethmac-ssid-policytagname**, and **ap-ethmac-ssid-sitetagname** keywords were introduced.

Usage Guidelines

Example

The following example shows how to configure a call station identifier sent in the RADIUS accounting messages:

```
Device(config)# radius-server attribute wireless accounting call-station-id site-tag-name
```

radius-server attribute wireless authentication call-station-id

To configure call station identifier sent in the RADIUS authentication messages, use the **radius-server attribute wireless authentication call-station-id** command. To remove the call station identifier from the radius accounting messages, use the **no** form of the command.

radius-server attribute wireless authentication call-station-id { **ap-ethmac-only** | **ap-ethmac-ssid** | **ap-ethmac-ssid-flexprofilename** | **ap-ethmac-ssid-policytagname** | **ap-ethmac-ssid-sitetagname** | **ap-group-name** | **ap-label-address** | **ap-label-address-ssid** | **ap-location** | **ap-macaddress** | **ap-macaddress-ssid** | **ap-macaddress-ssid-flexprofilename** | **ap-macaddress-ssid-policytagname** | **ap-macaddress-ssid-sitetagname** | **ap-name** | **ap-name-ssid** | **flex-profile-name** | **ipaddress** | **macaddress** | **policy-tag-name** | **site-tag-name** | **vlan-id** }

Syntax Description

ap-ethmac-only	Sets the call station identifier type to be AP's radio MAC address.
ap-ethmac-ssid	Sets the call station identifier type AP's radio MAC address with SSID.
ap-ethmac-ssid-flexprofilename	Sets the call station identifier type AP's radio MAC address with SSID and flex profile name.
ap-ethmac-ssid-policytagname	Sets the call station identifier type AP's radio MAC address with SSID and policy tag name.
ap-ethmac-ssid-sitetagname	Sets the call station identifier type AP's radio MAC address with SSID and site tag name.
ap-group-name	Sets the call station identifier type to use the AP group name.
ap-label-address	Sets the call station identifier type to the AP's radio MAC address that is printed on the AP label.
ap-label-address-ssid	Sets the call station identifier type to the AP's radio MAC address and SSID that is printed on the AP label.
ap-location	Sets the call station identifier type to the AP location.
ap-macaddress	Sets the call station identifier type to the AP's radio MAC address.
ap-macaddress-ssid	Sets the call station identifier type to the AP's radio MAC address with SSID.
ap-macaddress-ssid-flexprofilename	Sets the call station identifier type to the AP's radio MAC address with SSID and flex profile name.
ap-macaddress-ssid-policytagname	Sets the call station identifier type to the AP's radio MAC address with SSID and policy tag name.
ap-macaddress-ssid-sitetagname	Sets the call station identifier type to the AP's radio MAC address with SSID and site tag name.
ap-name	Sets the call station identifier type to the AP name.

ap-name-ssid	Sets the call station identifier type to the AP name with SSID.
flex-profile-name	Sets the call station identifier type to the flex profile name.
ipaddress	Sets the call station identifier type to the IP address of the system.
macaddress	Sets the call station identifier type to the MAC address of the system.
policy-tag-name	Sets the call station identifier type to the policy tag name.
site-tag-name	Sets the call station identifier type to the site tag name.
vlan-id	Sets the call station identifier type to the system's VLAN ID.

Command Default

Call station identifier is not configured.

Command Modes

Global Configuration(config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced.
Cisco IOS XE Bengaluru 17.4.1	This command was modified. The **policy-tag-name**, **flex-profile-name**, **ap-macaddress-ssid-flexprofilename**, **ap-macaddress-ssid-policytagname**, **ap-macaddress-ssid-sitetagname**, **ap-ethmac-ssid-flexprofilename**, **ap-ethmac-ssid-policytagname**, and **ap-ethmac-ssid-sitetagname** keywords were introduced.

Usage Guidelines

Example

The following example shows how to configure a call station identifier sent in the RADIUS authentication messages:

```
Device(config)# radius-server attribute wireless authentication call-station-id site-tag-name
```

range

To configure range from MAP to RAP bridge, use the **range** command.

range *range-in-feet*

Syntax Description

range-in-feet	Configure the range value in terms of feet. Valid range is from 150 feet to 132000 feet.

Command Default

1200

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 range from MAP to RAP bridge 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)# range 300
```

record wireless avc basic

To apply the *wireless avc basic* AVC flow record to a flow monitor, use the **record wireless avc basic** command.

record wireless avc basic

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.

Usage Guidelines This command specifies the basic wireless AVC template. When you are configuring AVC, you will need to create a flow monitor using the **record wireless avc basic** command.

Examples

The following example shows how to apply the *wireless avc basic* AVC flow record to a flow monitor named *test-flow*:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# flow monitor test-flow
Device(config-flow-monitor)# record wireless avc basic
```

redirect

To configure a redirect to an external portal, use the **redirect** command.

redirect {**for-login** | **on-failure** | **on-success** }*redirect-url-name*

Syntax Description

for-login	To login, redirect to this URL.
on-failure	If login fails, redirect to this URL.
on-success	If login is sucessful, redirect to this URL.
redirect-url-name	Redirect URL name.

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 an redirect to an external IPv4 URL to login:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# parameter-map type webauth parameter-name
Device(config-params-parameter-map)# redirect for-login cisco.com
```

redirect portal

To configure external IPv4 or IPv6 portal, use the **redirect portal** command.

redirect portal {**ipv4** | **ipv6** }*ip-addr*

Syntax Description

ipv4	IPv4 portal address
ipv6	IPv6 portal address

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 an external IPv4 portal address:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# parameter-map type webauth parameter-name
Device(config-params-parameter-map)# redirect portal ipv4 192.168.1.100
```

remote-lan

To map an RLAN policy profile to an RLAN profile, use the **remote-lan** command.

remote-lan *remote-lan-profile-name* **policy** *rlan-policy-profile-name* **port-id** *port-id*

Syntax Description

remote-lan-profile-name	Remote LAN profile name.
rlan-policy-profile-name	Remote LAN policy profile name.
port-id	Port ID.

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 map an RLAN policy profile to an RLAN profile:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless tag policy remote-lan-policy-tag
Device(config-policy-tag)# remote-lan rlan_profile_name policy rlan_policy_profile port-id
 2
Device(config-policy-tag)# end
```

rf tag

To configure an RF tag to the AP, use the **rf tag**command.

rf tag *rf-tag-name*

Syntax Description

rf-tag-name	RF tag name.

Command Default

None

Command Modes

config-ap-tag

Command History

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

Usage Guidelines

The AP will disconnect and rejoin after running this command.

Example

The following example shows how to configure an RF tag:

```
Device(config-ap-tag)# rf-tag rftag1
```

roaming-oi

To configure a 802.11u roaming organization identifier, use the **roaming-oi** command. To remove the roaming organization identifier, use the **no** form of the command.

roaming-oi *OI-value* [**beacon**]

Syntax Description

OI-value	Roaming organization identifier value.
beacon	Advertises the roaming organization identifier as part of the BSSID beacon.

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

You can configure up to 255 different OI values.

You can use a maximum of three beacons for roaming OIs.

If beacon is specified, the roaming OUI is advertised in the AP WLAN beacon or probe response, else it will only be returned while doing the roaming OUI ANQP query.

Example

The following example shows how to configure an operating class identifier:

```
Device(config)#wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# roaming-oi 24 beacon
```

rrc-evaluation

To configure Resource Reservation Control (RRC) reevaluation admission, use the **rrc-evaluation** command.

rrc-evaluation {**initial** | **periodic**}

Syntax Description

initial	Configures initial admission evaluation.
periodic	Configures periodic admission evaluation.

Command Default

None

Command Modes

config-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 the RRC reevaluation admission to initial admission evaluation.

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless media-stream group my-media-group 224.0.0.0 224.0.0.223
Device(config-media-stream)# rrc-evaluation initial
```

security

To configure mesh security, use the **security** command.

security { **eap** | **psk** }

Syntax Description

eap	Configure mesh security EAP for Mesh AP.
psk	Configure mesh security PSK for Mesh AP

Command Default

EAP

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 mesh security with EAP protcol on an Mesh AP:

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

security dot1x authentication-list

To configure security authentication list for IEEE 802.1x, use the **security dot1x authentication-list** *auth-list-name* command.

security dot1x authentication-list *auth-list-name*

Syntax Description

Parameter	Description
auth-list-name	Authentication list name.

Command Default

None

Command Modes

config-wlan

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 security authentication list for IEEE 802.1x:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan-name
Device(config-wlan)# security dot1x authentication-list auth-list-realm
```

security ft

To configure 802.11r fast transition parameters, use the **security ft** command. To configure fast transition **over the air**, use the **no security ft over-the-ds** command.

security ft [**over-the-ds** | **reassociation-timeout** *timeout-jn-seconds*]
no security ft [**over-the-ds** | **reassociation-timeout**]

Syntax Description

over-the-ds	(Optional) Specifies that the 802.11r fast transition occurs over a distributed system. The no form of the command with this parameter configures security ft over the air.
reassociation-timeout	(Optional) Configures the reassociation timeout interval.
timeout-in-seconds	(Optional) Specifies the reassociation timeout interval in seconds. The valid range is between 1 to 100. The default value is 20.

Command Default

The feature is disabled.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

None

WLAN Security must be enabled.

Example

The following example configures security FT configuration for an open WLAN:

```
Device#wlan test
Device(config-wlan)# client vlan 0140
Device(config-wlan)# no mobility anchor sticky
Device(config-wlan)# no security wpa
Device(config-wlan)# no security wpa akm dot1x
Device(config-wlan)# no security wpa wpa2
Device(config-wlan)# no security wpa wpa2 ciphers aes
Device(config-wlan)# security ft
Device(config-wlan)# shutdown
```

The following example shows a sample security FT on a WPA-enabled WLAN:

```
Device# wlan test
Device(config-wlan)# client vlan 0140
Device(config-wlan)# no security wpa akm dot1x
Device(config-wlan)# security wpa akm ft psk
Device(config-wlan)# security wpa akm psk set-key ascii 0 test-test
```

```
Device(config-wlan)# security ft
Device(config-wlan)# no shutdown
```

security pmf

To configure 802.11w Management Frame Protection (PMF) on a WLAN, use the **security pmf** command. To disable management frame protection, use the **no** form of the command.

security pmf {**association-comeback** *association-comeback-time-seconds* | **mandatory** | **optional** | **saquery-retry-time** *saquery-retry-time-milliseconds*}
no security pmf [**association-comeback** *association-comeback-time-seconds* | **mandatory** | **optional** | **saquery-retry-time** *saquery-retry-time-milliseconds*]

Syntax Description

association-comeback	Configures the 802.11w association comeback time.
association-comeback-time-seconds	Association comeback interval in seconds. Time interval that an associated client must wait before the association is tried again after it is denied with a status code 30. The status code 30 message is "Association request rejected temporarily; Try again later." The range is from 1 through 20 seconds.
mandatory	Specifies that clients are required to negotiate 802.1w PMF protection on the WLAN.
optional	Specifies that the WLAN does not mandate 802.11w support on clients. Clients with no 802.11w capability can also join.
saquery-retry-time	Time interval identified before which the SA query response is expected. If the device does not get a response, another SA query is tried.
saquery-retry-time-milliseconds	The saquery retry time in milliseconds. The range is from 100 to 500 ms. The value must be specified in multiples of 100 milliseconds.

Command Default

PMF is disabled.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

You must have WPA (Wi-Fi Protected Access) and AKM (Authentication Key Management) configured to use this feature. See Related Command section for more information on configuring the security parameters.

802.11w introduces an Integrity Group Temporal Key (IGTK) that is used to protect broadcast or multicast robust management frames. IGTK is a random value, assigned by the authenticator station (device) used to protect MAC management protocol data units (MMPDUs) from the source STA. The 802.11w IGTK key is

derived using the four-way handshake and is used only on WLANs that are configured with WPA2 security at Layer 2.

This example shows how to enable the association comeback value at 15 seconds.

```
Device(config-wlan)# security pmf association-comeback 15
```

This example shows how to configure mandatory 802.11w MPF protection for clients on a WLAN:

```
Device(config-wlan)# security pmf mandatory
```

This example shows how to configure optional 802.11w MPF protection for clients on a WLAN:

```
Device(config-wlan)# security pmf optional
```

This example shows how to configure the saquery parameter:

```
Device(config-wlan)# security pmf saquery-retry-time 100
```

This example shows how to disable the PMF feature:

```
Device(config-wlan)# no security pmf
```

security static-wep-key

To configure static WEP keys on a WLAN, use the **security static-wep-key** command.

security static-wep-key {**authentication** {**open** | **sharedkey** } | **encryption** {**104** | **40** } {**ascii** | **hex** | {**0** | **8** }*wep-key* | **wep-index** }}

Syntax Description

open	Open system authentication.
sharedkey	Shared key authentication.
0	Specifies an UNENCRYPTED password is used.
8	Specifies an AES encrypted password is used.
wep-key	Enter the name of the WEP key.

Command Default

None

Command Modes

config-wlan

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 authenticate 802.11 using shared key:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan profile-name wlan-id
Device(config-wlan)# security static-wep-key authentication sharedkey
```

security web-auth

To change the status of web authentication used on a WLAN, use the **security web-auth** command. To disable web authentication on a WLAN, use the **no** form of the command.

security web-auth [**authentication-list** *authentication-list-name* | **on-macfilter-failure** | **parameter-map** *parameter-map-name*]
no security web-auth [**authentication-list** [**authentication-list-name**] | **on-macfilter-failure** | **parameter-map** [**parameter-name**]]

Syntax Description

authentication-list *authentication-list-name*	Sets the authentication list for IEEE 802.1x.
on-macfilter-failure	Enables web authentication on MAC failure.
parameter-map *parameter-map-name*	Configures the parameter map.

Command Default

Web authentication is disabled.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1 Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Examples

The following example shows how to configure the authentication-list web authentication on a WLAN:

```
Device(config-wlan)# security web-auth authentication-list test
```

security wpa akm

To configure authentication key management using Cisco Centralized Key Management (CCKM), use the **security wpa akm** command. To disable the authentication key management for Cisco Centralized Key Management, use the **no** form of the command.

security wpa [**akm** { **cckm** | **dot1x** | **ft** | **pmf** | **psk** } | **wpa1** [**ciphers** { **aes** | **tkip** }] | **wpa2** [**ciphers** { **aes** }]]
no security wpa [**akm** { **cckm** | **dot1x** | **ft** | **pmf** | **psk** } | **wpa1** [**ciphers** { **aes** | **tkip** }] | **wpa2** [**ciphers** { **aes** }]]

Syntax Description

akm	Configures the Authentication Key Management (AKM) parameters.
aes	Configures AES (Advanced Encryption Standard) encryption support.
cckm	Configures Cisco Centralized Key Management support.
ciphers	Configures WPA ciphers.
dot1x	Configures 802.1x support.
ft	Configures fast transition using 802.11r.
pmf	Configures 802.11w management frame protection.
psk	Configures 802.11r fast transition pre-shared key (PSK) support.
tkip	Configures Temporal Key Integrity Protocol (TKIP) encryption support.
wpa2	Configures Wi-Fi Protected Access 2 (WPA2) support.

Command Default

By default Wi-Fi Protected Access2, 802.1x are enabled. WPA2, PSK, CCKM, FT dot1x, FT PSK, PMF dot1x, PMF PSK, FT Support are disabled. The FT Reassociation timeout is set to 20 seconds, PMF SA Query time is set to 200.

Command Modes

WLAN Configuration (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 CCKM on the WLAN.

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
Device(config)# wlan wlan1
Device(config-wlan)#security wpa akm cckm
```

server-uri

To configure the server Uniform Resource Identifier (URI) of an Online Sign-Up (OSU) operator, use the **server-uri** command. To remove the server URI, use the **no** form of the command.

server-uri *server-uri*

Syntax Description

server-uri	Server URI of an OSU operator.

Command Default

None

Command Modes

ANQP OSU Provider Configuration (config-anqp-osu-provider)

Command History

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

Example

The following example shows how to configure the server URI of an OSU operator:

```
Device(config-wireless-anqp-server)# osu-provider my-osu
Device(config-anqp-osu-provider)# server-uri yyyy
```

service-policy

To configure the quality of service (QoS) service policy, use the **service-policy** command. To disable a QoS policy, use the **no** form of this command.

service-policy { **client** | **input** | **output** } *policy-name*
no { **client** | **input** | **output** } *policy-name*

Syntax Description

client	Assigns a policy map to all clients in the WLAN.
input	Assigns an input policy map.
output	Assigns an output policy map.
policy-name	The policy map name.

Command Default

None

Command Modes

Wireless policy configuration

Command History

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

Examples

This example shows how to configure the input service policy:

```
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)# service-policy input test1
```

service-policy qos

To configure a QoS service policy, use the **service-policy qos** command.

service-policy qos {**input** | **output**}*policy-name*

Syntax Description

input	Input QoS policy.
output	Output QoS policy.
policy-name	Policy name.

Command Default

None

Command Modes

config-service-template

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 output QoS policy:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# service-template fabric-profile-name
Device(config-service-template)# service-policy qos output policy-name
```

service-template

To configure service template, use the **service-template** command.

service-template *service-template-name* {**access-group** *acl_list* | **vlan** *vlan_id* | **absolute-timer** *seconds* | **service-policy qos** {**input** | **output**}}

Syntax Description

service-template-name	Name of the service template.
acl_list	Access list name to be applied.
vlan_id	VLAN ID. The VLAN ID value ranges from 1 to 4094.
seconds	Session timeout value for service template. The session timeout value ranges from 1 to 65535 seconds.
service-policy qos {**input**	**output**	QoS policies for client.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

None

The following example shows how to configure service template:

```
Device#configure terminal
Device(config)#service-template cisco-phone-template
Device(config-service-template)#access-group foo-acl
Device(config-service-template)#vlan 100
Device(config-service-template)#service-policy qos input foo-qos
Device(config-service-template)#end
```

service timestamps

To configure the system to time-stamp debugging or logging messages, use the**service timestamps** command in global configuration commands. Use the **no** form of this command to disable this service.

service timestamps debug log {**datetime** | **uptime***localtimemsecshow-timezoneyear*}
no service timestamps debuglog

Syntax Description

debug	Debug as the timestamp message type.
log	Log as the timestamp message type.
datetime	**datetime**
uptime	(Optional) Time stamp with time since the system was rebooted.
localtime	(Optional) Time stamp relative to the local time zone.
msec	(Optional) Include milliseconds in the date and time stamp.
show-timezone	(Optional) Include the time zone name in the time stamp.
year	(Optional) Include year in timestamp.

Command Default

No time-stamping.

If **service timestamps** is specified with no arguments or keywords, default is **service timestamps debug uptime**.

The default for **service timestamps debugdatetime** is to format the time in UTC, with no milliseconds and no time zone name.

The command **no service timestamps** by itself disables time stamps for both debug and log messages.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.1.1s	This command was introduced in a release earlier than Cisco IOS XE Amsterdam 17.1.1s.

Usage Guidelines

Time stamps can be added to either debugging or logging messages independently. The uptime form of the command adds time stamps in the format HHHH:MM:SS, indicating the time since the system was rebooted. The datetime form of the command adds time stamps in the format MMM DD HH:MM:SS, indicating the date and time according to the system clock. If the system clock has not been set, the date and time are preceded by an asterisk (*) to indicate that the date and time are probably not correct.

Example

The following example enables time stamps on debugging messages, showing the time since reboot:

```
Device(config)# service timestamps debug uptime
```

The following example enables time stamps on logging messages, showing the current time and date relative to the local time zone, with the time zone name included:

```
Device(config)# service timestamps log datetime localtime show-timezone
```

session-timeout

To configure session timeout for clients associated to a WLAN, use the **session-timeout** command. To restore the default value, use the **no** form of this command.

session-timeout seconds
no session-timeout

Syntax Description

seconds	Timeout or session duration in seconds. The range is from 300 to 86400. The default value is 28,800. Configuring 86400 is equivalent to max timeout. And value 0 is not recommended.

Command Default

None

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1 Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

This example shows how to configure a session timeout to 3600 seconds:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#wireless profile policy policy1
Device(config-wireless-policy)#session-timeout 3600
```

set

To classify IP traffic by setting a Differentiated Services Code Point (DSCP) or an IP-precedence value in the packet, use the **set** command in policy-map class configuration mode. Use the **no** form of this command to remove traffic classification.

set
cos | **dscp** | **precedence** | **ip** | **qos-group** | **wlan**
set cos
{*cos-value* } | {**cos** | **dscp** | **precedence** | **qos-group** | **wlan**} [**table** *table-map-name*]
set dscp
{*dscp-value* } | {**cos** | **dscp** | **precedence** | **qos-group** | **wlan**} [**table** *table-map-name*]
set ip {**dscp** | **precedence**}
set precedence {*precedence-value* } | {**cos** | **dscp** | **precedence** | **qos-group**} [**table** *table-map-name*]
set qos-group
{*qos-group-value* | **dscp** [**table** *table-map-name*] | **precedence** [**table** *table-map-name*]}
set wlan user-priority
user-priority-value | **costable** *table-map-name* | **dscptable** *table-map-name* | **qos-grouptable** *table-map-name* | **wlantable** *table-map-name*

Syntax Description

cos	Sets the Layer 2 class of service (CoS) value or user priority of an outgoing packet. You can specify these values:
	• *cos-value*—CoS value from 0 to 7. You also can enter a mnemonic name for a commonly used value.
	• Specify a packet-marking category to set the CoS value of the packet. If you also configure a table map for mapping and converting packet-marking values, this establishes the "map from" packet-marking category. Packet-marking category keywords:
	  • **cos**—Sets a value from the CoS value or user priority.
	  • **dscp**—Sets a value from packet differentiated services code point (DSCP).
	  • **precedence**—Sets a value from packet precedence.
	  • **qos-group**—Sets a value from the QoS group.
	  • **wlan**—Sets the WLAN user priority values.
	• (Optional)**table** *table-map-name*—Indicates that the values set in a specified table map are used to set the CoS value. Enter the name of the table map used to specify the CoS value. The table map name can be a maximum of 64 alphanumeric characters.
	If you specify a packet-marking category but do not specify the table map, the default action is to copy the value associated with the packet-marking category as the CoS value. For example, if you enter the **set cos precedence** command, the precedence (packet-marking category) value is copied and used as the CoS value.

dscp	Sets the differentiated services code point (DSCP) value to mark IP(v4) and IPv6 packets. You can specify these values:
	• *cos-value*—Number that sets the DSCP value. The range is from 0 to 63. You also can enter a mnemonic name for a commonly used value.
	• Specify a packet-marking category to set the DSCP value of the packet. If you also configure a table map for mapping and converting packet-marking values, this establishes the "map from" packet-marking category. Packet-marking category keywords:
	  • **cos**—Sets a value from the CoS value or user priority.
	  • **dscp**—Sets a value from packet differentiated services code point (DSCP).
	  • **precedence**—Sets a value from packet precedence.
	  • **qos-group**—Sets a value from the QoS group.
	  • **wlan**—Sets a value from WLAN.
	• (Optional)**table** *table-map-name*—Indicates that the values set in a specified table map will be used to set the DSCP value. Enter the name of the table map used to specify the DSCP value. The table map name can be a maximum of 64 alphanumeric characters.
	If you specify a packet-marking category but do not specify the table map, the default action is to copy the value associated with the packet-marking category as the DSCP value. For example, if you enter the **set dscp cos** command, the CoS value (packet-marking category) is copied and used as the DSCP value.

ip	Sets IP values to the classified traffic. You can specify these values: • **dscp**—Specify an IP DSCP value from 0 to 63 or a packet marking category. • **precedence**—Specify a precedence-bit value in the IP header; valid values are from 0 to 7 or specify a packet marking category.

precedence	Sets the precedence value in the packet header. You can specify these values:
	• *precedence-value*— Sets the precedence bit in the packet header; valid values are from 0 to 7. You also can enter a mnemonic name for a commonly used value.
	• Specify a packet marking category to set the precedence value of the packet.
	  • **cos**—Sets a value from the CoS or user priority.
	  • **dscp**—Sets a value from packet differentiated services code point (DSCP).
	  • **precedence**—Sets a value from packet precedence.
	  • **qos-group**—Sets a value from the QoS group.
	• (Optional)**table** *table-map-name*—Indicates that the values set in a specified table map will be used to set the precedence value. Enter the name of the table map used to specify the precedence value. The table map name can be a maximum of 64 alphanumeric characters.
	If you specify a packet-marking category but do not specify the table map, the default action is to copy the value associated with the packet-marking category as the precedence value. For example, if you enter the **set precedence cos** command, the CoS value (packet-marking category) is copied and used as the precedence value.

qos-group	Assigns a QoS group identifier that can be used later to classify packets. • *qos-group-value*—Sets a QoS value to the classified traffic. The range is 0 to 31. You also can enter a mnemonic name for a commonly used value. • **dscp**—Sets the original DSCP field value of the packet as the QoS group value. • **precedence**—Sets the original precedence field value of the packet as the QoS group value. • (Optional)**table** *table-map-name*—Indicates that the values set in a specified table map will be used to set the DSCP or precedence value. Enter the name of the table map used to specify the value. The table map name can be a maximum of 64 alphanumeric characters. If you specify a packet-marking category (**dscp** or **precedence**) but do not specify the table map, the default action is to copy the value associated with the packet-marking category as the QoS group value. For example, if you enter the **set qos-group precedence** command, the precedence value (packet-marking category) is copied and used as the QoS group value.

wlan user-priority *wlan-user-priority*	Assigns a WLAN user-priority to the classified traffic. You can specify these values: • *wlan-user-priority*—Sets a WLAN user priority to the classified traffic. The range is 0 to 7. • **cos**—Sets the Layer 2 CoS field value as the WLAN user priority. • **dscp**—Sets the DSCP field value as the WLAN user priority. • **precedence**—Sets the precedence field value as the WLAN user priority. • **wlan**—Sets the WLAN user priority field value as the WLAN user priority. • (Optional)**table** *table-map-name*—Indicates that the values set in a specified table map will be used to set the WLAN user priority value. Enter the name of the table map used to specify the value. The table map name can be a maximum of 64 alphanumeric characters. If you specify a packet-marking category but do not specify the table map, the default action is to copy the value associated with the packet-marking category as the WLAN user priority. For example, if you enter the **set wlan user-priority cos** command, the cos value (packet-marking category) is copied and used as the WLAN user priority.

Command Default

No traffic classification is defined.

Command Modes

Policy-map class configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1 Cisco IOS XE Gibraltar 16.12.1	This command was i

Usage Guidelines

For the **set dscp** *dscp-value* command, the **set cos** *cos-value* command, and the **set ip precedence** *precedence-value* command, you can enter a mnemonic name for a commonly used value. For example, you can enter the **set dscp af11** command, which is the same as entering the **set dscp 10** command. You can enter the **set ip precedence critical** command, which is the same as entering the **set ip precedence 5** command. For a list of supported mnemonics, enter the **set dscp ?** or the **set ip precedence ?** command to see the command-line help strings.

When you configure the **set dscp cos**command, note the following: The CoS value is a 3-bit field, and the DSCP value is a 6-bit field. Only the three bits of the CoS field are used.

When you configure the **set dscp qos-group** command, note the following:

- The valid range for the DSCP value is a number from 0 to 63. The valid value range for the QoS group is a number from 0 to 99.
- If a QoS group value falls within both value ranges (for example, 44), the packet-marking value is copied and the packets is marked.
- If QoS group value exceeds the DSCP range (for example, 77), the packet-marking value is not be copied and the packet is not marked. No action is taken.

The **set qos-group** command cannot be applied until you create a service policy in policy-map configuration mode and then attach the service policy to an interface or ATM virtual circuit (VC).

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

Examples

This example shows how to assign DSCP 10 to all FTP traffic without any policers:

```
Device(config)# policy-map policy_ftp
Device(config-pmap)# class-map ftp_class
Device(config-cmap)# exit
Device(config)# policy policy_ftp
Device(config-pmap)# class ftp_class
Device(config-pmap-c)# set dscp 10
Device(config-pmap)# exit
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

sftp-image-path (image-download-mode sftp)

To configure the image path of the SFTP server for image download, use the **sftp-image-path** command. Use the **no** form of the command to negate the command or to set the command to its default.

`sftp-image-path`*sftp-image-path*

`no sftp-image-path`*sftp-image-path*

Syntax Description

sftp-image-path	Specifies the image path of the SFTP server.

Command Default

None

Command Modes

Wireless image download profile SFTP configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

```
Device(config)# wireless profile image-download default
Device(config-wireless-image-download-profile)# image-download-mode sftp
Device(config-wireless-image-download-profile-sftp)# sftp-image-path
/download/object/stream/images/ap-images
```

sftp-image-server (image-download-mode sftp)

To configure the SFTP server address for image download, use the **sftp-image-server** command. Use the **no** form of this command to negate the configuration or to set the command to its default.

```
sftp-image-server {A.B.C.D | X:X:X:X::X}

no sftp-image-server {A.B.C.D | X:X:X:X::X}
```

Syntax Description

A.B.C.D	Specifies the SFTP IPv4 server address.
X:X:X:X::X	Specifies the SFTP IPv6 server address.

Command Default

None

Command Modes

Wireless image download profile SFTP configuration mode.

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

```
Device(config)# wireless profile image-download default
Device(config-wireless-image-download-profile)# image-download-mode sftp
Device(config-wireless-image-download-profile-sftp)# sftp-image-server 10.1.1.1
```

sftp-password (image-download-mode sftp)

To configure the SFTP server password for image dowload, use the **sftp-password** command. Use the **no** form of this command to negate the configuration or to set the command to its default.

```
sftp-password {0| 8}<Enter password> <Re-enter password>

no sftp-password {0 | 8}<Enter password> <Re-enter password>
```

Syntax Description

0	Specifies that an unencrypted password will follow.
8	Specifies that an AES encrypted password will follow.
password	Specifies the SFTP server password.
re-enter password	Indicates that the user must re-enter the SFTP server password.

Command Default

None

Command Modes

Wireless image download profile SFTP configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

```
Device(config)# wireless profile image-download default
Device(config-wireless-image-download-profile)# image-download-mode sftp
Device(config-wireless-image-download-profile-sftp)# sftp-password 0 xxxxxxxx
```

sftp-password (trace-export)

To configure the SFTP server password for trace export, use the **sftp-password** command. Use the **no** form of this command to negate the configuration or to set the command to its default.

`sftp-password<`*Enter password*`> <`*Re-enter password*`>`

`no sftp-password<`*Enter password*`> <`*Re-enter password*`>`

Syntax Description

password	Specifies the SFTP server password.
re-enter password	Indicates that the user must re-enter the SFTP server password.

Command Default

None

Command Modes

Wireless trace export profile SFTP configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

```
Device(config)# wireless profile transfer trace-export trace_export_name
Device(config-wireless-trace-export-profile)# log-export-mode sftp
Device(config-wireless-trace-export-profile-sftp)# sftp-password xxxxxxxx xxxxxxxx
```

sftp-path

To configure the path at the SFTP server for trace log export, use the **sftp-path** command. Use the **no** form of the command to negate the command or to set the command to its default.

`sftp-path`*sftp-path*

`no sftp-path`*sftp-path*

Syntax Description

sftp-path	Specifies the path at the SFTP server.

Command Default

None

Command Modes

Wireless trace export profile SFTP configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

```
Device(config)# wireless profile transfer trace-export trace_export_name
Device(config-wireless-trace-export-profile)# log-export-mode sftp
Device(config-wireless-trace-export-profile-sftp)# sftp-path
/download/object/stream/images/ap-images
```

sftp-server

To configure the SFTP server address for trace export, use the **sftp-server** command. Use the **no** form of this command to negate the configuration or to set the command to its default.

```
sftp-server{A.B.C.D | X:X:X:X::X}

no sftp-server {A.B.C.D | X:X:X:X::X}
```

Syntax Description

A.B.C.D	Specifies the SFTP IPv4 server address.
X:X:X:X::X	Specifies the SFTP IPv6 server address.

Command Default

None

Command Modes

Wireless trace export profile SFTP configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

```
Device(config)# wireless profile transfer trace-export trace_export_name
Device(config-wireless-trace-export-profile)# log-export-mode sftp
Device(config-wireless-trace-export-profile-sftp)# sftp-server 10.1.1.1
```

sftp-username (image-download-mode sftp)

To configure the SFTP server username for image download, use the **sftp-username**command. Use the **no** form of this command to negate the configuration or to set the command to its default.

`sftp-username` *Username*

`no sftp-username` *Username*

Syntax Description

username	Specifies the SFTP server username.

Command Default

None

Command Modes

Wireless image download profile SFTP configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

```
Device(config)# wireless profile image-download default
Device(config-wireless-image-download-profile)# image-download-mode sftp
Device(config-wireless-image-download-profile-sftp)# sftp-username sftp-server-username
```

sftp-username (trace-export)

To configure the SFTP server username for trace export, use the **sftp-username**command. Use the **no** form of this command to negate the configuration or to set the command to its default.

`sftp-username` *Username*

`no sftp-username` *Username*

Syntax Description

username	Specifies the SFTP server username.

Command Default

None

Command Modes

Wireless trace export profile SFTP configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

```
Device(config)# wireless profile transfer trace-export trace_export_name
Device(config-wireless-trace-export-profile)# log-export-mode sftp
Device(config-wireless-trace-export-profile-sftp)# sftp-username sftp-server-username
```

snmp-server enable traps wireless

To enable wireless notifications for a host, use the **snmp-server enable traps wireless** command.

snmp-server enable traps wireless [**AP** | **bsnMobileStation** | **MESH** | **bsnAutoRF** | **rogue** | **wireless_mobility** | **RRM** | **bsnGeneral**]

Syntax Description

AP	Enables wireless SNMP traps for APs
bsnMobileStation	Enables wireless client traps
MESH	Enables wireless mesh traps
bsnAutoRF	Enables wireless RF related traps
rogue	Enables traps for wireless rogue
wireless_mobility	Enables traps for wireless mobility
RRM	Enables traps for wireless RRM
bsnGeneral	Enables general controller traps

Command Default

None

Command Modes

Global Configuration (config)

Command History

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

Examples

The following example shows how to enable wireless notifications for a host:

```
Device# snmp-server enable traps wireless MESH
```

snmp-server group

To configure a new Simple Network Management Protocol (SNMP) group, use the **snmp-server group** command in global configuration mode. To remove a specified SNMP group, use the **no** form of this command.

snmp-server group *group-name* {**v1** | **v2c** | **v3** } [**access** [**ipv6** *named-access-list*] [*acl-numberacl-name*]] [**context** *context-name*] [**notify** *notify-view*] [**read** *read-view*] [**write** *write-view*]
no snmp-server group *group-name* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**context** *context-name*]

Syntax Description

group-name	Name of the group.
v1	Specifies that the group is using the SNMPv1 security model. SNMPv1 is the least secure of the possible SNMP security models.
v2c	Specifies that the group is using the SNMPv2c security model. The SNMPv2c security model allows informs to be transmitted and supports 64-character strings.
v3	Specifies that the group is using the SNMPv3 security model. SMNPv3 is the most secure of the supported security models. It allows you to explicitly configure authentication characteristics.
context	(Optional) Specifies the SNMP context to associate with this SNMP group and its views.
context-name	(Optional) Context name.
read	(Optional) Specifies a read view for the SNMP group. This view enables you to view only the contents of the agent.
read-view	(Optional) String of a maximum of 64 characters that is the name of the view. The default is that the read-view is assumed to be every object belonging to the Internet object identifier (OID) space (1.3.6.1), unless the **read** option is used to override this state.
write	(Optional) Specifies a write view for the SNMP group. This view enables you to enter data and configure the contents of the agent.
write-view	(Optional) String of a maximum of 64 characters that is the name of the view. The default is that nothing is defined for the write view (that is, the null OID). You must configure write access.
notify	(Optional) Specifies a notify view for the SNMP group. This view enables you to specify a notify, inform, or trap.

notify-view	(Optional) String of a maximum of 64 characters that is the name of the view. By default, nothing is defined for the notify view (that is, the null OID) until the **snmp-server host** command is configured. If a view is specified in the **snmp-server group** command, any notifications in that view that are generated will be sent to all users associated with the group (provided a SNMP server host configuration exists for the user). Cisco recommends that you let the software autogenerate the notify view. See the "Configuring Notify Views" section in this document.
access	(Optional) Specifies a standard access control list (ACL) to associate with the group.
ipv6	(Optional) Specifies an IPv6 named access list. If both IPv6 and IPv4 access lists are indicated, the IPv6 named access list must appear first in the list.
named-access-list	(Optional) Name of the IPv6 access list.
acl-number	(Optional) The *acl-number*argument is an integer from 1 to 99 that identifies a previously configured standard access list.
acl-name	(Optional) The *acl-name* argument is a string of a maximum of 64 characters that is the name of a previously configured standard access list.

Command Default

No SNMP server groups are configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.1.1s	This command was introduced in a release earlier than Cisco IOS XE Amsterdam 17.1.1s.

Usage Guidelines

When a community string is configured internally, two groups with the name public are autogenerated, one for the v1 security model and the other for the v2c security model. Similarly, deleting a community string will delete a v1 group with the name public and a v2c group with the name public.

No default values exist for authentication or privacy algorithms when you configure the **snmp-server group** command. Also, no default passwords exist. For information about specifying a Message Digest 5 (MD5) password, see the documentation of the **snmp-server user** command.

Configuring Notify Views

The notify-view option is available for two reasons:

- If a group has a notify view that is set using SNMP, you may need to change the notify view.
- The **snmp-server host** command may have been configured before the **snmp-server group** command. In this case, you must either reconfigure the **snmp-server host** command, or specify the appropriate notify view.

Specifying a notify view when configuring an SNMP group is not recommended, for the following reasons:

- The **snmp-server host** command autogenerates a notify view for the user, and then adds it to the group associated with that user.

- Modifying the group's notify view will affect all users associated with that group.

Instead of specifying the notify view for a group as part of the **snmp-server group** command, use the following commands in the order specified:

1. **snmp-server user** --Configures an SNMP user.
2. **snmp-server group** --Configures an SNMP group, without adding a notify view .
3. **snmp-server host** --Autogenerates the notify view by specifying the recipient of a trap operation.

SNMP Contexts

SNMP contexts provide VPN users with a secure way of accessing MIB data. When a VPN is associated with a context, that VPN's specific MIB data exists in that context. Associating a VPN with a context enables service providers to manage networks with multiple VPNs. Creating and associating a context with a VPN enables a provider to prevent the users of one VPN from accessing information about users of other VPNs on the same networking device.

Use this command with the **context** *context-name* keyword and argument to associate a read, write, or notify SNMP view with an SNMP context.

Create an SNMP Group

The following example shows how to create the SNMP server group "public," allowing read-only access for all objects to members of the standard named access list "lmnop":

```
Device(config)# snmp-server group public v2c access lmnop
```

Remove an SNMP Server Group

The following example shows how to remove the SNMP server group "public" from the configuration:

```
Device(config)# no snmp-server group public v2c
```

Associate an SNMP Server Group with Specified Views

The following example shows SNMP context "A" associated with the views in SNMPv2c group "GROUP1":

```
Device(config)# snmp-server context A
Device(config)# snmp mib community commA
Device(config)# snmp mib community-map commA context A target-list commAVpn
Device(config)# snmp-server group GROUP1 v2c context A read viewA write viewA notify viewB
```

snmp-server subagent cache

To prevent CPU spikes in the controller during Simple Network Management Protocol (SNMP) polling, use the **snmp-server subagent cache** command. To disable the subagent cache, use the **no** form of this command.

snmp-server subagent cache [**timeout** *seconds*]

snmp-server subagent cache [**timeout** *seconds*]

Syntax Description

timeout	Specifies the subagent cache timeout.
seconds	The server timeout value, in seconds. The valid values range from 1 to 100, with a default of 60.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Dublin 17.11.1	This command was introduced.

Usage Guidelines

Use this command to prevent CPU spikes in the controller by clearing the cache at regular intervals.

Examples

The following example shows how to prevent CPU spikes in the controller during SNMP polling:

```
Device# configure terminal
Device(config)# snmp-server subagent cache
```

ssid broadcast persistent

To enable the SSID broadcast mode, use the **ssid broadcast persistent** command. Use the **no** form of the command to disable the feature.

ssid broadcast persistent

no ssid broadcast persistent

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

AP profile configuration (config-ap-profile)

Command History

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

Usage Guidelines

Enabling or disabling this feature causes the AP to re-join.

Examples

The following example shows how to enable the SSID broadcast mode:

```
Device# configure terminal
Device(config)# ap profile ap-profile-name
Device(config-ap-profile)# ssid broadcast persistent
```

stopbits

To configure the stop bits for the console port, use the **stopbits** command. To revert to the default values, use the **no** form of this command.

stopbits { *1* | *2* }

no stopbits { *1* | *2* }

Syntax Description

1	Specifies one stop bit.
2	Specifies two stop bits.

Command Default

1 stop bit

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

You can configure the console ports only from a session on the console port.

Examples

The following example shows how to configure the stop bits for the console port:

```
Device# configure terminal
Device(config)# line console 0
Device(config-line)# stopbits 1
```

strong-network-key

To enable strong password evaluation for network key, use the **strong-network-key**command.

strong-network-key

Syntax Description

This command has no keywords or arguments.

Command Modes

Wireless URWB profile configuration (config-wireless-urwb-profile)

Command History

Release	Modification
Cisco IOS XE 17.18.1	This command was introduced.

Examples

The following example shows how to enable strong password evaluation for network key:

```
Device# configure terminal
Device(config)# wireless profile urwb urwb-profile-name
Device(config-wireless-urwb-profile)# strong-network-key
```

tag rf

To configure a policy tag for an AP filter, use the **tag rf** command.

tag rf *rf-tag*

Syntax Description

rf-tag	RF tag name.

Command Default

None

Command Modes

config-ap-filter

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 policy tag for an AP filter:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap filter name ap-filter-name
Device(config-ap-filter)# rf tag rf-tag-name
```

tag site

To configure a site tag for an AP filter, use the **tag site** *site-tag* command.

tag site *site-tag*

Syntax Description		
	site-tag	Name of the site tag.

Command Default None

Command Modes config-ap-filter

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 site tag for an AP filter:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap filter name ap-filter-name
Device(config-ap-filter)# site tag site-tag-name
```

tftp-image-path (image-download-mode tftp)

To configure the image path at the TFTP server for image download, use the **tftp-image-path** command. Use the **no** form of this command to negate the configuration or to set the command to its default.

`tftp-image-path` *tftp-image-path*

`no tftp-image-path` *tftp-image-path*

Syntax Description

tftp-image-path	Specifies the image path of the TFTP server.

Command Default

None

Command Modes

Wireless image dowload profile TFTP configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

```
Device(config)# wireless profile image-download default
Device(config-wireless-image-download-profile)# image-download-mode tftp
Device(config-wireless-image-download-profile-tftp)# tftp-image-path
/download/object/stream/images/ap-images
```

tftp-image-server (image-download-mode tftp)

To configure the TFTP server address for image download, use the **tftp-image-server** command. Use the **no** form of this command to negate the configuration or to set the command to its default.

```
image-download-mode tftp

tftp-image-server {A.B.C.D | X:X:X:X::X}

no tftp-image-server {A.B.C.D | X:X:X:X::X}
```

Syntax Description

A.B.C.D	Specifies the TFTP IPv4 server address.
X:X:X:X::X	Specifies the TFTP IPv6 server address.

Command Default

None

Command Modes

Wireless image download profile TFTP configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

```
Device(config)# wireless profile image-download default
Device(config-wireless-image-download-profile)# image-download-mode tftp
Device(config-wireless-image-download-profile-tftp)# tftp-image-server 10.1.1.1
```

tftp-path

To configure the path at the TFTP server for trace log export, use the **tftp-path** command. Use the **no** form of the command to negate the command or to set the command to its default.

`tftp-path`*tftp-path*

`no tftp-path`*tftp-path*

Syntax Description

tftp-path	Specifies the path at the TFTP server.

Command Default

None

Command Modes

Wireless trace export profile TFTP configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

```
Device(config)# wireless profile transfer trace-export trace_export_name
Device(config-wireless-trace-export-profile)# log-export-mode tftp
Device(config-wireless-trace-export-profile-tftp)# tftp-path
/download/object/stream/images/ap-images
```

tftp-server

To configure the TFTP server address for trace export, use the **tftp-server** command. Use the **no** form of this command to negate the configuration or to set the command to its default.

```
tftp-server {A.B.C.D | X:X:X:X::X}

no tftp-server {A.B.C.D | X:X:X:X::X}
```

Syntax Description

A.B.C.D	Specifies the TFTP IPv4 server address.
X:X:X:X::X	Specifies the TFTP IPv6 server address.

Command Default

None

Command Modes

Wireless trace export profile TFTP configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

```
Device(config)# wireless profile transfer trace-export trace_export_name
Device(config-wireless-trace-export-profile)# log-export-mode tftp
Device(config-wireless-trace-export-profile-tftp)# tftp-server 10.1.1.1
```

udp-timeout

To configure timeout value for UDP sessions, use the **udp-timeout** command.

udp-timeout *timeout_value*

Syntax Description

timeout_value	Is the timeout value for UDP sessions. The range is from 1 to 30 seconds. **Note** The *public-key* and *resolver* parameter-map options are automatically populated with the default values. So, you need not change them.

Command Default

None

Command Modes

Profile configuration

Command History

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

Example

This example shows how to configure timeout value for UDP sessions:

```
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)# udp-timeout 2
Device(config-profile)# end
```

umbrella-param-map

To configure the Umbrella OpenDNS feature for WLAN, use the **umbrella-param-map** command.

umbrella-param-map *umbrella-name*

Syntax Description

umbrella-name

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 the Umbrella OpenDNS feature for WLAN:

```
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)# umbrella-param-map global
Device(config-wireless-policy)# end
```

update-timer

To configure the mDNS update timers for flex profile, use the **update-timer** command. To disable the command, use the **no** form of this command.

update-timer { **service-cache** *<1-100>* | **statistics** *<1-100>* }

update-timer { **service-cache** *<1-100>* | **statistics** *<1-100>* }

Syntax Description

update-timer	Configures the mDNS update timers for flex profile.
service-cache *<1-100>*	Specifies the mDNS update service-cache timer for flex profile. The default value is one minute,
statistics *<1-100>*	Specifies the mDNS update statistics timer for flex profile. The default value is one minute,

Command Default

None

Command Modes

mDNS flex profile configuration

Command History

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

Examples

The following example shows how to configure the mDNS update timers for flex profile:

```
Device(config-mdns-flex-prof)# update-timer service-cache 20
```

urwb chan-list channel

To configure the channel list for mobility and DFS backup, use the **urwb chan-list channel** *channel-num* **cwidth** {**160MHz** | **20MHz** | **40MHz** | **80MHz**} command. Use the **no** form of this command to disable the feature.

urwb chan-list channel *channel-num* **cwidth** { **160MHz** | **20MHz** | **40MHz** | **80MHz** }

urwb chan-list channel *channel-num* **cwidth** { **160MHz** | **20MHz** | **40MHz** | **80MHz** }

Syntax Description

channel-num	Specifes the channel number.
cwidth	Specifies the channel width.
160MHz	Specifies the channel width as 160MHz.
20MHz	Specifies the channel width as 20MHz
40MHz	Specifies the channel width as 40MHz
80MHz	Specifies the channel width as 80MHz

Command Default

None

Command Modes

Wireless radio profile configuration (config-wireless-radio-profile)

Command History

Release	Modification
Cisco IOS XE 17.18.1	This command was introduced.

Examples

The following example shows how to configure the channel list for mobility and DFS backup:

```
Device# configure terminal
Device(config)# wireless profile radio radio-profile-name
Device(config-wireless-radio-profile)# urwb chan-list channel 100 cwidth 40MHz
```

urwb channel

To configure the URWB radio channel, use the **urwb channel 5ghz** *channel-number*

urwb channel 5ghz *channel-number (1-233)*

Syntax Description

channel-number	Specifies the channel number of the URWB radio. The channel number range is from 1 to 233.

Command Default

None

Command Modes

Wireless radio profile configuration (config-wireless-radio-profile)

Command History

Release	Modification
Cisco IOS XE 17.18.1	This command was introduced.

Examples

The following example shows how to configure the URWB radio channel:

```
Device# configure terminal
Device(config)# wireless profile radio radio-profile-name
Device(config-wireless-radio-profile)# urwb channel 5ghz 100
```

urwb crypto policy

To configure AES-based encryption policy, use the **urwb crypto policy** { **fixed-key** | **none** | **rotating-key**} command.

urwb crypto policy { **fixed-key** | **none** | **rotating-key** }

Syntax Description

fixed	Enables AES-based encryption with fixed key.
none	Disable AES-based encryption.
rotating-key	Enables AES-based encryption with rotating key.

Command Default

None

Command Modes

Wireless radio profile configuration (config-wireless-radio-profile)

Command History

Release	Modification
Cisco IOS XE 17.18.1	This command was introduced.

Examples

The following example shows how to AES-based encryption policy:

```
Device# configure terminal
Device(config)# wireless profile radio radio-profile-name
Device(config-wireless-radio-profile)# urwb crypto policy fixed
```

urwb crypto rotating-key-timeout

To configure AES-based encryption rotating-key timeout, use the **urwb crypto rotating-key-timeout** *timeout* command. Use the **no** form of this command to disable the feature.

urwb crypto rotating-key-timeout *timeout*

no urwb crypto rotating-key-timeout *timeout*

Syntax Description

timeout	Specifes the rotating-key timeout in seconds. The range is from 0 to 65535.

Command Default

The default value is 15 seconds.

Command Modes

Wireless radio profile configuration (config-wireless-radio-profile)

Command History

Release	Modification
Cisco IOS XE 17.18.1	This command was introduced.

Examples

The following example shows how to configure AES-based encryption rotating-key timeout:

```
Device# configure terminal
Device(config)# wireless profile radio radio-profile-name
Device(config-wireless-radio-profile)# urwb crypto rotating-key-timeout 15
```

urwb cwidth

To configure the URWB channel width, use the **urwb cwidth** {**160MHz** | **20MHz** | **40MHz** | **80MHz**}. Use the **no** form of this command to disable this feature.

urwb cwidth { **160MHz** | **20MHz** | **40MHz** | **80MHz** }

no urwb cwidth

Syntax Description

160MHz	Configures the radio channel width as 160MHz.
20MHz	Configures radio channel width as 20MHz.
40MHz	Configures radio channel width as 40MHz.
80MHz	Configure radio channel width as 80MHz.

Command Default

None

Command Modes

Wireless radio profile configuration (config-wireless-radio-profile)

Command History

Release	Modification
Cisco IOS XE 17.18.1	This command was introduced.

Examples

The following example shows how to configure the URWB radio channel width:

```
Device# configure terminal
Device(config)# wireless profile radio radio-profile-name
Device(config-wireless-radio-profile)# urwb cwidth 40MHz
```

urwb-profile

Syntax Description

Command Default

Command Modes

Command History

Release	Modification

Usage Guidelines

Task ID

Task ID	Operation

Example

urwb ptmp autoscan

To configure the URWB point-to-multi-point (PTMP) automatic scan, use the **urwb ptmp autoscan** command. Use the **no** form of this command to disable the feature.

urwb ptmp autoscan

no urwb ptmp autoscan

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Wireless radio profile configuration (config-wireless-radio-profile)

Command History

Release	Modification
Cisco IOS XE 17.18.1	This command was introduced.

Usage Guidelines

This setting is applicable only if the URWB role is set to point-to-multi-point and if the URWB PTMP role is secondary.

Examples

The following example shows how to configure the URWB point-to-multi-point (PTMP) automatic scan

```
Device# configure terminal
Device(config)# wireless profile radio radio-profile-name
Device(config-wireless-radio-profile)# urwb ptmp autoscan
```

urwb ptmp cluster-id

To configure the URWB point-to-multi-point (PTMP) cluster ID, use the **urwb ptmp cluster-id** *cluster-id* command. Use the **no** form of this command to disable the feature.

urwb ptmp cluster-id *cluster-id*

no urwb ptmp cluster-id *cluster-id*

Syntax Description

cluster-id	Specifes the ID of the cluster.

Command Default

None

Command Modes

Wireless radio profile configuration (config-wireless-radio-profile)

Command History

Release	Modification
Cisco IOS XE 17.18.1	This command was introduced.

Usage Guidelines

When more than one point-to-multi-point cluster operates in the same location, each cluster can be logically separated from every other cluster by using a cluster ID value that is unique to that cluster. A Fixed client radio only communicates wirelessly with a Fixed Base radio that shares the same cluster ID.

This setting is applicable only if the URWB role is set to point-to-multi-point.

Examples

The following example shows how to configure the URWB point-to-multi-point (PTMP) cluster ID:

```
Device# configure terminal
Device(config)# wireless profile radio radio-profile-name
Device(config-wireless-radio-profile)# urwb ptmp cluster-id ptmp-cluster
```

urwb ptmp rssi-threshold

To configure the URWB point-to-multi-point (PTMP) RSSI threshold at which a scan for new Principal units are triggered, use the **urwb ptmp rssi-threshold** *threshold-value* command. Use the **no** form of this command to disable the feature.

urwb ptmp rssi-threshold *threshold-value*

no urwb ptmp rssi-threshold *threshold-value*

Syntax Description

threshold-value	Specifes the RSSI threshold value. The range is from 1 to 100.

Command Default

None

Command Modes

Wireless radio profile configuration (config-wireless-radio-profile)

Command History

Release	Modification
Cisco IOS XE 17.18.1	This command was introduced.

Examples

The following example shows how to configure the URWB point-to-multi-point (PTMP) RSSI threshold:

```
Device# configure terminal
Device(config)# wireless profile radio radio-profile-name
Device(config-wireless-radio-profile)# urwb ptmp rssi-threshold 3
```

urwb ptmp tower-id

To configure the URWB point-to-multi-point (PTMP) tower ID, use the **urwb ptmp tower-id** *tower-id* command. Use the **no** form of this command to disable the feature.

urwb ptmp tower-id *tower-id*

no urwb ptmp tower-id *tower-id*

Syntax Description

tower-id	Specifes the ID of the tower.

Command Default

None

Command Modes

Wireless radio profile configuration (config-wireless-radio-profile)

Command History

Release	Modification
Cisco IOS XE 17.18.1	This command was introduced.

Usage Guidelines

Tower ID: To avoid connectivity issues when multiple towers are serving the same cluster, the tower-id parameter can be enabled on base radios. All radios mounted on the same tower share the same tower ID. Even if two base radios see each other through a physical link and wirelessly, they know that they are on a different tower and will continue to advertise themselves.

When a client is connected to one tower (Tower 1) and moves close to another one (Tower 2), it automatically connects to a new base on Tower 2. This gives a wider coverage area and continuous connectivity. The same tower design, with different tower IDs, can be replicated to provide more coverage zones.

This setting is applicable only if URWB role is set to point-to-multi-point and if URWB PTMP role is Fixed Base.

Examples

The following example shows how to configure the URWB point-to-multi-point (PTMP) tower ID:

```
Device# configure terminal
Device(config)# wireless profile radio radio-profile-name
Device(config-wireless-radio-profile)# urwb ptmp tower-id tower1
```

urwb role

To configure the URWB role associated radio slot, use the **urwb role** {**fixed** | **mobility** | **point-to-multi-point**}

urwb role { **fixed** | **mobility** | **point-to-multi-point** }

Syntax Description

fixed	Configures the radio role as fixed.
mobility	Configures the radio role as mobility.
point-to-multi-point	Configures the radio role as point-to-multi-point.

Command Default

None

Command Modes

Wireless radio profile configuration (config-wireless-radio-profile)

Command History

Release	Modification
Cisco IOS XE 17.18.1	This command was introduced.

Examples

The following example shows how to configure the URWB mobility role:

```
Device# configure terminal
Device(config)# wireless profile radio radio-profile-name
Device(config-wireless-radio-profile)# urwb role fixed
```

username

To add a user who can access the Cisco Catalyst 9800 Series Controller using SSH, use the **username** command in configuration mode. If the user already exists, the password, the privilege level, or both change with this command. To delete the user from the system, use the **no** form of this command.

[no] username *username* **password** {**hash** | **plain**} *password* **role** {**admin** | **user**] [**disabled** [**email** email-address]] [**email** email-address]

For an existing user, use the following command option:

username username **password role** {admin | **user**} password

Syntax Description

username	You should enter only one word which can include hyphen (-), underscore (_) and period (.). **Note** Only alphanumeric characters are allowed at an initial setup.
password	The command to use specify password and user role.
password	Password character length up to 40 alphanumeric characters. You must specify the password for all new users.
hash | plain	Type of password. Up to 34 alphanumeric characters.
role admin | user	Sets the privilege level for the user.
disabled	Disables the user according to the user's email address.
email *email-address*	The user's email address. For example, user1@example.com.
wlan-profile-name	Displays details of the WLAN profile.

Command Default

The initial user during setup.

Command Modes

Configuration

Usage Guidelines

The **username** command requires that the username and password keywords precede the hash | plain and the admin | user options.

Example 1

```
ncs/admin(config)# username admin password hash ###### role admin
ncs/admin(config)#
```

Example 2

```
ncs/admin(config)# username admin password plain Secr3tp@swd role admin
ncs/admin(config)#
```

Example 3

```
ncs/admin(config)# username admin password plain Secr3tp@swd role admin email
admin123@example.com
ncs/admin(config)#
```

venue

To configure a 802.11u venue information, use the **venue** command. To remove the venue, use the **no** form of the command.

venue *venue-name language-code* [*venue-url*]

Syntax Description

venue-name	Name of the venue. Should not exceed 220 characters.
language-code	A three character language code for the operator. Use only the first three letters of the language, in lower case, for the language code. For example, use *eng* for English. To see the full list of language codes, go to: http://www.loc.gov/standards/iso639-2/php/code_list.php.
venue-url	URL of the venue.

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 802.11u venue information:

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# venue test eng cisco.com
```

violation

To configure stream violation policy on periodic reevaluation, use the **violation** command.

violation {**drop** | **fallback**}

Syntax Description

Parameter	Description
drop	Stream will be dropped on periodic reevaluation.
fallback	Stream will be demoted to BestEffort class on periodic reevaluation.

Command Default

None

Command Modes

config-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 stream violation policy on periodic reevaluation:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless media-stream group my-media-group 224.0.0.0 224.0.0.223
Device(config-media-stream)# violation drop
```

wan-metrics

To configure Hotspot 2.0 WAN metrics, use the **wan-metrics** command. Use the **no** form of the command to remove the WAN.

wan-metrics
{**downlink-load**|**downlink-speed**|**full-capacity-link**|**link-status**{**down**|**not-configured**|**test-state**|**up**}|**load-measurement-duration**|**uplink-load**|**uplink-speed**}

Syntax Description

downlink-load	Sets the WAN downlink load. Valid range is from 0-255. Values are scaled linearly with 255 representing 100 percent.
downlink-speed	Sets the WAN downlink speed, in kbps. Valid range is from 0-4294967295.
full-capacity-link	Operates WAN link at its maximum capacity.
link-status	Sets the WAN link status. Options are: • **down**: Link down • **not-configured**: Link is not configured. • **test-state**: Link is in test state. • **up**: Link is up.
load-measurement-duration	Sets the duration of the uplink or downlink load measurement. Valid range is from 0-65535.
uplink-load	Sets the WAN uplink load. Valid range is from 0-255. Values are scaled linearly with 255 representing 100 percent.
uplink-speed	Sets the WAN uplink speed, in kbps. Valid range is from 0-4294967295.

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 Hotspot 2.0 WAN uplink speed:

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# wan-metrics uplink-load 23
```

wgb broadcast-tagging

To configure WGB broadcast tagging for a wireless policy profile, use the **wgb broadcast-tagging** command.

wgb broadcast-tagging

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 enable WGB broadcast tagging for a wireless policy profile:

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

wgb vlan

To configure WGB VLAN client support for a WLAN policy profile, use the **wgb vlan** command.

wgb vlan

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 enable WGB VLAN client support for the WLAN policy profile named *wlan1-policy-profile*:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy wlan1-policy-profile
Device(config-wireless-policy)# wgb vlan
```

whitelist acl

To configure the whitelist ACL, use the **whitelist acl** command.

whitelist acl {*standard_acl_value* | *extended_acl_value* | *acl_name*}

Syntax Description

standard_acl_value	Specifies the standard access list. Range is from 1 to 199.
extended_acl_value	Specifies the extended access list. Range is from 1300 to 2699.
acl_name	Specifies the named access list.

Command Default

None

Command Modes

ET-Analytics configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1 Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

This example shows how to enable in-active timer 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)# whitelist acl
eta-whitelist
Device((config-et-analytics)# ip access-list
extended eta-whitelist
Device(config-ext-nacl)# permit udp any any eq tftp
Device(config-ext-nacl)# end
```

wired-vlan-range

To configure wired VLANs on which mDNS service discovery should take place, use the **wired-vlan-range** command. To disable the command, use the **no** form of this command.

wired-vlan-range *wired-vlan-range-value*

Syntax Description

wired-vlan-range	Configures wired VLANs on which mDNS service discovery should take place.
wired-vlan-range-value	Specifies the wired VLAN range value.

Command Default

None

Command Modes

mDNS flex profile configuration

Command History

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

Examples

The following example shows how to configure wired VLANs on which mDNS service discovery should take place:

```
Device(config-mdns-flex-prof)# wired-vlan-range range-value
```

config wlan assisted-roaming

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

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

Syntax Description

neighbor-list	Configures an 802.11k neighbor list for a WLAN.
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.
prediction	Configures an assisted roaming optimization prediction for a WLAN.
enable	Enables the configuration on the WLAN.
disable	Disables the configuration on the WLAN.
wlan_id	Wireless LAN identifier between 1 and 512 (inclusive).

Command Default

The 802.11k neighbor list is enabled for all WLANs.

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

Usage Guidelines

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

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

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

wireless aaa policy

To configure a wireless AAA policy, use the **wireless aaa policy** command.

wireless aaa policy *aaa-policy*

Syntax Description

aaa-policy	Name of the wireless AAA policy.

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 a wireless AAA policy named *aaa-policy-test*

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

wireless aaa policy

To configure a new AAA policy, use the **wireless aaa policy** command.

wireless aaa policy *aaa-policy-name*

Syntax Description

aaa-policy-name	AAA policy name.

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 a AAA policy name:

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

wireless autoqos policy-profile

To enable the **autoqos** wireless policy with an executable command, use the autoqos command. Use the **disable** command to disable wireless AutoQos.

wireless autoqos policy-profile*policy-profile-name* **default_policy_profile mode** { **clear** | **enterprise-avc** | **fastlane** | **guest** | **voice** }

wireless autoqos disable

Syntax Description

autoqos	Configures wireless Auto QoS.
mode	Specifies the wireless AutoQoS mode.
enterprise-avc	Enables AutoQos wireless enterprise AVC policy.
clear	Clears the configured wireless policy.
fastlane	Enables the AutoQos fastlane policy. This will disable and enable the 2.4GHz or 5GHz 802.11 network.
guest	Enables AutoQos wireless guest policy.
voice	Enables AutoQos wireless voice policy. This will disable and enable the 2.4GHz or 5GHz 802.11 network.

Command Default

None

Command Modes

Privilege EXEC mode

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

This example shows how to enable AutoQoS wireless enterprise policy:

```
Device# wireless autoqos policy-profile default-policy-profile mode enterprise-avc
```

wireless broadcast vlan

To enable broadcast support on a VLAN, use the **wireless broadcast vlan** command in global configuration mode. To disable Ethernet broadcast support, use the **no** form of the command.

wireless broadcast vlan [*vlan-id*]
no wireless broadcast vlan [*vlan-id*]

Syntax Description

vlan-id	(Optional) Specifies the VLAN ID to enable broadcast support to that VLAN. The value ranges from 1 to 4095.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1 Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

Use this command in the global configuration mode only.

This example shows how to enable broadcasting on VLAN 20:

```
Device(config)# wireless broadcast vlan 20
```

wireless client

To configure client parameters, use the **wireless client** command in global configuration mode.

wireless client {**association limit** *assoc-number* **interval** *interval* | **band-select** {**client-mid-rssi** *rssi* | **client-rssi** *rssi* | **cycle-count** *count* | **cycle-threshold** *threshold* | **expire dual-band** *timeout* | **expire suppression** *timeout*} | **fast-ssid-change** | **max-user-login** *max-user-login* | **notification** {**interval** *time* | **join-failure aaathreshold***percentage* | **roam-failure threshold** *percentage*} | **timers auth-timeout** *seconds* | **user-timeout** *user-timeout*}

Syntax Description

association limit *assoc-number* **interval** *interval*	Enables association request limit per access point slot at a given interval and configures the association request limit interval. You can configure number of association request per access point slot at a given interval from one through 100. You can configure client association request limit interval from 100 through 10000 milliseconds.
band-select	Configures the band select options for the client.
client-mid-rssi *rssi*	Sets the client mid-rssi threshold for band select. The minimum dBm of a client RSSI to respond to probe is between -90 and -20.
client-rssi *rssi*	Sets the client received signal strength indicator (RSSI) threshold for band select. The minimum dBm of a client RSSI to respond to probe is between -90 and -20.
cycle-count *count*	Sets the band select probe cycle count. You can configure the cycle count from 1 to 10.
cycle-threshold *threshold*	Sets the time threshold for a new scanning cycle. You can configure the cycle threshold from 1 to 1000 milliseconds.
expire dual-band *timeout*	Sets the timeout before stopping to try to push a given client to the 5-GHz band. You can configure the timeout from 10 to 300 seconds, and the default value is 60 seconds.
expire suppression *timeout*	Sets the expiration time for pruning previously known dual-band clients. You can configure the suppression from 10 to 200 seconds, and the default timeout value is 20 seconds.
fast-ssid-change	Enables the fast SSID change for mobile stations.
max-user-login *max-user-login*	Configures the maximum number of login sessions for a user.

notification	Configures notifications.
interval *time*	Configures notifications for an interval. The valid time ranges from 1 to 1440 seconds.
join-failure aaa threshold *percentage*	Configures notifications for client join failures. You can configure the threshold percentage to trigger an alert. The valid threshold percentage ranges from 1 to 100.
roam-failure threshold *percentage*	Configures notifications for client roam failures. You can configure the threshold for notifications. The valid threshold percentage ranges from 1 to 100.
timers auth-timeout *seconds*	Configures the client timers.
user-timeout *user-timeout*	Configures the idle client timeout.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

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

This example shows how to set the proble cycle count for band select to 8:

```
Device# configure terminal
Device(config)# wireless client band-select cycle-count 8
Device(config)# end
```

This example shows how to set the time threshold for a new scanning cycle with threshold value of 700 milliseconds:

```
Device# configure terminal
Device(config)# wireless client band-select cycle-threshold 700
Device(config)# end
```

This example shows how to suppress dual-band clients from the dual-band database after 70 seconds:

```
Device# configure terminal
Device(config)# wireless client band-select expire suppression 70
Device(config)# end
```

wireless client mac-address

To configure the wireless client settings, use the **wireless client mac-address** command in global configuration mode.

wireless client mac-address *mac-addr* **ccx** {**clear-reports** | **clear-results** | **default-gw-ping** | **dhcp-test** | **dns-ping** | **dns-resolve hostname** *host-name* | **get-client-capability** | **get-manufacturer-info** | **get-operating-parameters** | **get-profiles** | **log-request** {**roam** | **rsna** | **syslog**} | **send-message** *message-id* | **stats-request** *measurement-duration* {**dot11** | **security**} | **test-abort** | **test-association** *ssid bssid dot11 channel* | **test-dot1x** [*profile-id*] *bssid dot11 channel* | **test-profile** {**any***profile-id*}}

Syntax Description

mac-addr	MAC address of the client.
ccx	Cisco client extension (CCX).
clear-reports	Clears the client reporting information.
clear-results	Clears the test results on the controller.
default-gw-ping	Sends a request to the client to perform the default gateway ping test.
dhcp-test	Sends a request to the client to perform the DHCP test.
dns-ping	Sends a request to the client to perform the Domain Name System (DNS) server IP address ping test.
dns-resolve hostname *host-name*	Sends a request to the client to perform the Domain Name System (DNS) resolution test to the specified hostname.
get-client-capability	Sends a request to the client to send its capability information.
get-manufacturer-info	Sends a request to the client to send the manufacturer's information.
get-operating-parameters	Sends a request to the client to send its current operating parameters.
get-profiles	Sends a request to the client to send its profiles.
log-request	Configures a CCX log request for a specified client device.
roam	(Optional) Specifies the request to specify the client CCX roaming log
rsna	(Optional) Specifies the request to specify the client CCX RSNA log.
syslog	(Optional) Specifies the request to specify the client CCX system log.

send-message *message-id*

Sends a message to the client.

Message type that involves one of the following:

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

- 30—Scheduled maintenance period.
- 31—The WLAN security method is not correct.
- 32—The WLAN encryption method is not correct.
- 33—The WLAN authentication method is not correct.

stats-request *measurement-duration*	Senda a request for statistics.
dot11	Optional) Specifies dot11 counters.
security	(Optional) Specifies security counters.
test-abort	Sends a request to the client to abort the current test.
test-association *ssid bssid dot11 channel*	Sends a request to the client to perform the association test.
test-dot1x	Sends a request to the client to perform the 802.1x test.
profile-id	(Optional) Test profile name.
bssid	Basic SSID.
dot11	Specifies the 802.11a, 802.11b, or 802.11g network.
channel	Channel number.
test-profile	Sends a request to the client to perform the profile redirect test.
any	Sends a request to the client to perform the profile redirect test.
profile-id	Test profile name. **Note** The profile ID should be from one of the client profiles for which client reporting is enabled.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1 Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

The **default-gw-ping** test does not require the client to use the diagnostic channel.

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

```
Device# configure terminal
Device(config)# wireless client mac-address 00:1f:ca:cf:b6:60 ccx clear-reports
Device(config)# end
```

wireless client vlan-persistent

To enable client roaming across different policy profiles, use the **wireless client vlan-persistent** command.

wireless client vlan-persistent

no wireless client vlan-persistent

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 17.3.1	This command was introduced.

Examples

The following example shows how to enable client roaming across different policy profiles:

```
Device(config) # wireless client vlan-persistent
```

wireless config validate

To validate whether the wireless configuration is complete and consistent (all the functional profiles and tags are defined, and all the associations are complete and consistent), use the **wireless config validate** command in privileged EXEC mode.

wireless config validate

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.

Usage Guidelines

In Cisco vEWLC, the wireless configuration is built using a collection of profiles, with each profile defining a functional block. These functional blocks are defined independently and is used to realize well-defined associations through intent based work-flows in building the wireless LAN. Such flexibility of modularizing the functional blocks requires the administrator to ensure that all associations are consistent and complete.

To ensure completeness and consistency of the wireless configuration, a configuration validation library is used to validate the configuration definitions across tables. The **wireless config validate** exec command is introduced from this release to validate the wireless configuration and report inconsistencies, if any, using contextual error message that is visible in btrace infra and on the console (if console logging is enabled). This command calls out any inconsistencies (unresolved associations) enabling you to realize a functional wireless LAN.

Use the following command to direct the output to a file: **show logging | redirect bootflash:** *filename* .

The following set of wireless configurations are validated:

RF tag	Site tag	Policy tag	Policy profile	Flex profile
site-tag	flex-profile	wlan profile	IPv4 ACL name	VLAN ACL
poliy-tag	ap-profile	policy profile	Fabric name	ACL-policy
rf-tag	-—	-—	service-policy input and output name	RF Policy (5GHz and 24GHz)
-—	-—	-—	service-policy input and client output name	-—

Example

The following is sample output from the **wireless config validate** command

```
Device# wireless config validate

Oct 10 18:21:59.576 IST: %CONFIG_VALIDATOR_MESSAGE-5-EWLC_GEN_ERR: Chassis 1 R0/0: wncmgrd:
 Error in AP: fc99.473e.0a90  Applied site-tag : mysite definitiondoes not exist
Oct 10 18:21:59.576 IST: %CONFIG_VALIDATOR_MESSAGE-5-EWLC_GEN_ERR: Chassis 1 R0/0: wncmgrd:
 Error in AP: fc99.473e.0a90  Applied policy-tag : mypolicy definition does not exist
Oct 10 18:21:59.576 IST: %CONFIG_VALIDATOR_MESSAGE-5-EWLC_GEN_ERR: Chassis 1 R0/0: wncmgrd:
 Error in AP: fc99.473e.0a90  Applied rf-tag : myrf definition does not exist
```

wireless country

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

wireless country *country-code*

Syntax Description

country-code	Two-letter country code.

Command Default

None

Command Modes

Global configuration

Command History

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

Usage Guidelines

The Cisco 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 code on the device to IN (India):

```
Device(config)# wireless country IN
```

wireless exclusionlist mac address

To manually add clients to the exclusionlist, use the wireless exclusion list command. To remove the manual entry, use the no form of the command.

wireless exclusionlist *mac_address* **description**

Syntax Description

description *value*	Configures the entry description.

Command Default

None

Command Modes

Global Configuration

Command History

Cisco IOS XE Gibraltar 16.10.1	Modification
	This command was introduced in this release.

Usage Guidelines

If a client was added to the exclusion list dynamically, the command to remove it is **wireless client mac-address xxxx.xxxx.xxxx deauthenticate** from enable mode.

Example

This example shows how to manage exclusion entries:

```
Device(config)# wireless exclusion list xxxx.xxxx.xxxx
```

wireless hotspot anqp-server

To configure a wireless Hotspot 2.0 Access Network Query Protocol (ANQP) server, use the **wireless hotspot anqp-server** command. To disable the Hotspot 2.0 server, use the **no** form of the command.

wireless hotspot anqp-server *server-name*

Syntax Description

server-name	Name of the Hotspot 2.0 ANQP server.

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 a Hotspot 2.0 ANQP server:

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

wireless hotspot gas-rate-limit

To limit the maximum number of Generic Advertisement Services (GAS) or Access Network Query Protocol (ANQP) requests processed per second, use the **wireless hotspot gas-rate-limit** command. To disable the limit, use the **no** form of the command.

wireless hotspot gas-rate-limit *limit*

Syntax Description

limit	Number of GAS or ANQP requests to process, per second. Valid range is from 1-2500.

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 limit the maximum number of GAS or ANQP requests processed per second:

```
Device(config)# wireless hotspot gas-rate-limit 100
```

wireless hotspot icon

To configure an icon for Hotspot 2.0, use the **wireless hotspot icon** command. To remove the icon, use the **no** form of the command.

wireless hotspot icon {**bootflash:filename** | **flash:filename**} *media-type language-code icon-width icon-height*

Syntax Description

media-type	Media type for this icon file. **Note** The icon file should match the types defined in: http://www.iana.org/assignments/media-types/index.html
language-code	A three character language code for the operator. Use only the first three letters of the language, in lower case, for the language code. For example, use *eng* for English. To see the full list of language codes, go to: http://www.loc.gov/standards/iso639-2/php/code_list.php.
icon-width	Icon width, in pixels. Valid range is from 0-65535.
icon-height	Icon height, in pixels. Valid range is from 0-65535.

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 an icon for Hotspot 2.0:

```
Device(config)# wireless hotspot icon flash:test jpeg en 655 400
```

wireless ipv6 ra wired

To enable the forwarding of Router Advertisement message to the wired clients, use the **wireless ipv6 ra wired** command.

wireless ipv6 ra wired { **nd** { **na-forward** | **ns-forward** } | **ra-wired** }

Syntax Description

nd	Configures wireless IPv6 ND parameters.
na-forward	Enables forwarding of Neighbor Advertisement to wireless clients.
ns-forward	Enable forwarding of Neighbor Solicitation to wireless clients.
ra	Configures wireless IPv6 Router Advertisement parameters.
wired	Enables forwarding of Router Advertisement message to the wired clients.

Command Default

None

Command Modes

Global Configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.3	This command was introduced.

Example

The following example shows how to enable the forwarding of Router Advertisement message to the wired clients:

```
Device(config)# wireless ipv6 ra wired
```

Warning The **wireless ipv6 ra wired** command must be enabled only for certification purpose and not during the deployment.

wireless load-balancing

To globally configure aggressive load balancing on the controller, use the **wireless load-balancing** command in global configuration mode.

wireless load-balancing {**denial** *denial-count* | **window** *client-count*}

Syntax Description

denial *denial-count*	Specifies the number of association denials during load balancing. Maximum number of association denials during load balancing is from 1 to 10 and the default value is 3.
window *client-count*	Specifies the aggressive load balancing client window, with the number of clients needed to trigger aggressive load balancing on a given access point. Aggressive load balancing client window with the number of clients is from 0 to 20 and the default value is 5.

Command Default

Disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1 Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

Load-balancing-enabled WLANs do not support time-sensitive applications like voice and video because of roaming delays.

When you use Cisco 7921 and 7920 Wireless IP Phones with controllers, make sure that aggressive load balancing is disabled on the voice WLANs for each controller. Otherwise, the initial roam attempt by the phone might fail, causing a disruption in the audio path.

This example shows how to configure association denials during load balancing:

```
Device# configure terminal
Device(config)# wireless load-balancing denial 5
Device(config)# end
```

wireless macro-micro steering transition-threshold

To configure micro-macro transition thresholds, use the **wireless macro-micro steering transition-threshold** command.

wireless macro-micro steering transition-threshold {**balancing-window** | **client count** *number-clients* } {**macro-to-micro** | **micro-to-macro** *RSSI in dBm*}

Syntax Description

balancing-window	Active instance of the configuration in Route-processor slot 0.
client	Standby instance of the configuration in Route-processor slot 0.
number-clients	Valid range is 0 to 65535 clients.
macro-to-micro	Configures the macro to micro transition RSSI.
micro-to-macro	Configures micro-macro client load balancing window.
RSSI in dBm	RSSI in dBm. Valid range is –128 to 0.

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 balancing-window:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless macro-micro steering transition-threshold balancing-window
number-of-clients
```

wireless macro-micro steering probe-suppression

To configure micro-macro probe suppressions, use the **wireless macro-micro steering probe-suppression** command.

wireless macro-micro steering probe-suppression {**aggressiveness** *number-of-cycles* | | **hysteresis***RSSI in dBm* | **probe-auth** | **probe-only**}

Syntax Description

aggressiveness	Configures probe cycles to be suppressed. The number of cycles range between 0 - 255.
hysteresis	Indicate show much greater the signal strength of a neighboring access point must be in order for the client to roam to it. The RSSI decibel value ranges from -6 to -3.
probe-auth	Enables mode to suppress probes and single auth
probe-only	Enables mode to suppress only probes

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.1	This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.12.1.

Examples

The following example shows how to configure balancing-window:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless macro-micro steering probe-suppression aggressiveness
number-of-cycles
```

wireless management certificate

To create a wireless management certificate details, use the **wireless management certificate** command.

wireless management certificate ssc {**auth-token** {**0** | **8**} *token* | **trust-hash** *hash-key* }

Syntax Description

auth-token	Authentication token.
token	Token name.
trust-hash	Trusted SSC hash list.
hash-key	SHA1 fingerprint.
0	Specifies an UNENCRYPTED token.
8	Specifies an AES encrypted token.

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.

Example

The following example shows how to configure a wireless management certificate:

```
Device# configure terminal
Device(config)# wireless management certificate ssc trust-hash test
```

wireless management interface

To create a wireless management interface, use the **wireless management interface** command.

wireless management interface { **GigabitEthernet** | **Loopback** | **Vlan** } *interface-number*

Syntax Description

interface-number	Interface number.

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.

Example

The following example shows how to configure a wireless management interface:

```
Device# configure terminal
Device(config)# wireless management interface vlan vlan1
```

wireless management trustpoint

To create a wireless management trustpoint, use the **wireless management trustpoint** command.

wireless management trustpoint *trustpoint-name*

Syntax Description

trustpoint-name	Trustpoint name.

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

Use this command only on the Cisco Catalyst 9800 Wireless Controller for Cloud platform and not on appliances as the appliances use the SUDI certificate by default without the need for this command.

Example

The following example shows how to configure a wireless management trustpoint:

```
Device# configure terminal
Device(config)# wireless management trustpoint test
```

wireless ewc-ap ap ap-type

To convert a single AP to CAPWAP or to embedded wireless controller, use the **wireless ewc-ap ap ap-type** command.

wireless ewc-ap ap ap-type *Cisco-AP-name* { **capwap** | **ewc** }

Syntax Description

ewc-ap	Configures the embedded wireless controller parameters.
ap-type	Configures the AP parameter.
Cisco-AP-name	Indicates the name of the Cisco AP.
capwap	Changes to Capwap ap-type.
ewc	Changes to the embedded wireless controller ap-type.

Command Default

None

Command Modes

Privileged EXEC mode

Command History

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

Example

The following example shows how to convert a single AP to a CAPWAP ap-type or a embedded wireless controller ap-type:

```
Device#wireless ewc-ap ap ap-type ap_name {capwap | ewc}
```

wireless ewc-ap ap capwap

To specify the CAPWAP parameters for an AP, use the **wireless ewc-ap ap capwap** command.

wireless ewc-ap ap capwap *Primary-Controller-Name* { **A.B.C.D** | **X:X:X:X::X** }

Syntax Description

ewc-ap	Configures the embedded wireless controller parameters.
capwap	Configures the CAPWAP parameters.
Primay-Controller-Name	Indicates the name of the controller.
A.B.C.D	Indicates the IPv4 address of the primary controller.
X:X:X:X::X	Indicates the IPv6 address of the primary controller.

Command Default

None

Command Modes

Privileged EXEC mode

Command History

Release	Modification
Cisco IOS XE 16.12.1	This message was introduced.

Example

The following example shows how to specify the CAPWAP parameters for an AP:

```
Device#wireless ewc-ap ap capwap controller_name {10.1.1.1 | 9:0:0:0::1}
```

wireless ewc-ap ap reload

To reload the embedded wireless controller AP, use the **wireless ewc-ap ap reload** command.

wireless ewc-ap ap reload

Syntax Description

ewc-ap	Configures the embedded wireless controller parameters.
reload	Reloads the embedded wireless controller AP.

Command Default

None

Command Modes

Privileged EXEC mode

Command History

Release	Modification
Cisco IOS XE 16.12.1	This message was introduced.

Example

The following example shows how to reload the embedded wireless controller AP:

```
Device#wireless ewc-ap ap reload
```

wireless ewc-ap ap shell

To access the AP parameters on the embedded wireless controller AP shell, use the **wireless ewc-ap ap shell** command.

wireless ewc-ap ap shell { **chassis** { *chassis-number* | **active** | **standby** } **R0** | **username** }

Syntax Description

chassis	Specifies the chassis.
chassis-number	Specifies the chassis number as either 1 or 2.
active	Configures the active instance in route processor slot 0.
standby	Configures the standby instance in route processor slot 0.
R0	Specifies the route processor in slot 0.
username	Specifies the AP management username.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

```
Device#wireless ewc-ap ap shell chassis 1 R0
```

wireless ewc-ap ap shell username

To configure the AP management username on the embedded wireless controller AP shell, use the **wireless ewc-ap ap shell username** command.

wireless ewc-ap ap shell username *username* **chassis** { *chassis-number* | **active** | **standby** } **R0**

Syntax Description

chassis	Specifies the chassis.
chassis-number	Specifies the chassis number as either 1 or 2.
active	Configures the active instance in route processor slot 0.
standby	Configures the standby instance in route processor slot 0.
R0	Specifies the route processor in slot 0.
username	Specifies the AP management username.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

```
Device#wireless ewc-ap ap shell username username1 chassis 1 R0
```

wireless ewc-ap preferred-master

To select the standby controller when the network is up and running, use the **wireless ewc-ap preferred-master** command.

wireless ewc-ap preferred-master *AP-name*

Syntax Description

ewc-ap	Configures the embedded wireless controller parameters.
preferred-master	Configures the preferred primary AP.
AP-name	Indicates the name of the preferred primary AP.

Command Default

None

Command Modes

Global configuration (config)

Command History

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

Example

The following example shows how to set a preferred primary ap-type:

```
Device(config)#wireless ewc-ap preferred-master AP-name
```

wireless ewc-ap factory-reset

To perform factory reset on the embedded wireless controller and on all the access points connected to the controller, use the **wireless ewc-ap factory-reset** command.

wireless ewc-ap factory-reset

Syntax Description

ewc-ap	Configures the embedded wireless controller parameters .
factory-reset	Resets Cisco AP configuration to factory default.

Command Default

None

Command Modes

Privileged EXEC mode

Command History

Release	Modification
Cisco IOS XE 16.12.1	This command was introduced.

Example

The following example shows how to factory-reset the embedded wireless controller network:

```
Device#wireless ewc-ap factory-reset
```

wireless ewc-ap vrrp vrid

To configure the embedded wireless controller VRRP network identifier, use the **wireless ewc-ap vrrp vrid** command.

wireless ewc-ap vrrp vrid*value <1-255>*

Syntax Description

ewc-ap	Configures the embedded wireless controller parameters.
vrrp	Configires the preferred primary APembedded wireless controller VRRP.
vrid	Indicates the VRRP VRID. Values are from 1-255. The default value is 1.
value	Indicates the VRRP VRID value.

Command Default

None

Command Modes

Global configuration mode

Command History

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

Example

The following example shows how to configure the VRRP network identifier:

```
Device#wireless ewc-ap vrrp vrid 1
```

wireless profile calender-profile name

To configure a calendar profile, use the **wireless profile calender-profile name** command.

wireless profile calender-profile name *name*

Syntax Description

name	Specifies the name of the calendar profile.

Command Default

None

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

This example shows how to configure a calendar profile:

```
Device# configure terminal
Device(config)# wireless profile calender-profile name daily_calendar_profile
Device(config-calender-profile)# start 09:00:00 end 17:00:00
Device(config-calender-profile)# recurrance daily
Device(config-calender-profile)# end
```

wireless profile image-download default

To configure the default image download profile for AP Join Download and Predownload, use the following command:

Note **Default** is the only profile name that you can enter.

wireless profile image-download default

Syntax Description

wireless profile	Configures the wireless profile parameters.
image-download	Configures the EWC-AP image download parameters.
default	Specifies the profile name - default. Default is the only profile name that you can enter.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

```
Device# wireless profile image-download default
```

wireless profile policy

To configure WLAN policy profile, use the **wireless profile policy** command.

wireless profile policy *policy-profile*

Syntax Description

policy-profile	Name of the WLAN policy profile.

Command Default

The default profile name is default-policy-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 a WLAN policy profile:

```
Device(config)# wireless profile policy mywlan-profile-policy
```

wireless profile transfer

To configure the export of trace logs on the embedded wireless controller, use the **wireless profile transfer** command. Use the **no** form of this command to negate the command or to set the command to its default.

[**no**] **wireless profiletransfertrace-export** *trace-export-profile-name*

Syntax Description

trace-export	Configures the trace export parameters.
trace-export-profile-name	Specifies the trace export profile name.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.12.2s	This command was introduced.

Example

```
Device# wireless profile transfer trace-export trace-export-profile-name
```

wireless profile urwb

To configure the URWB profile, use the **wireless profile urwb** command in the global configuration mode.

wireless profile urwb

Syntax Description

urwb-profile-name	Specifies the URWB profile name.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 17.18.1	This command was introduced.

Examples

The following example shows how to configure the URWB profile:

```
Device# configure terminal
Device(config)# wireless profile urwb urwb-profile-name
```

wireless rfid

To set the static radio-frequency identification (RFID) tag data timeout value, use the **wireless rfid** command in global configuration mode.

wireless rfid timeout *timeout-value*

Syntax Description

timeout	Configures the static RFID tag data timeout value.
timeout-value	RFID tag data timeout value. Valid values range from 60-7200.

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 set the static RFID tag data timeout value.

```
Device(config)# wireless rfid timeout 70
```

wireless security dot1x

To configure IEEE 802.1x global configurations, use the **wireless security dot1x** command.

wireless security dot1x [**eapol-key** {**retries** *retries* | **timeout** *milliseconds*} | **group-key interval** *sec* | **identity-request** {**retries** *retries* | **timeout** *seconds*} | **radius** [**call-station-id**] {**ap-macaddress** | **ap-macaddress-ssid** | **ipaddress** | **macaddress**} | **request** {**retries** *retries* | **timeout** *seconds*} | **wep key** {**index 0** | **index 3**}]

Syntax Description

eapol-key	Configures eapol-key related parameters.
retries *retries*	(Optional) Specifies the maximum number of times (0 to 4 retries) that the controller retransmits an EAPOL (WPA) key message to a wireless client. The default value is 2.
timeout *milliseconds*	(Optional) Specifies the amount of time (200 to 5000 milliseconds) that the controller waits before retransmitting an EAPOL (WPA) key message to a wireless client using EAP or WPA/WPA-2 PSK. The default value is 1000 milliseconds.
group-key interval *sec*	Configures EAP-broadcast key renew interval time in seconds (120 to 86400 seconds).
identity-request	Configures EAP ID request related parameters.
retries *retries*	(Optional) Specifies the maximum number of times (0 to 4 retries) that the controller request the EAP ID. The default value is 2.
timeout *seconds*	(Optional) Specifies the amount of time (1 to 120 seconds) that the controller waits before retransmitting an EAP Identity Request message to a wireless client. The default value is 30 seconds.
radius	Configures radius messages.
call-station-id	(Optional) Configures Call-Station Id sent in radius messages.
ap-macaddress	Sets Call Station Id Type to the AP's MAC Address.
ap-macaddress-ssid	Sets Call Station Id Type to 'AP MAC address':'SSID'.
ipaddress	Sets Call Station Id Type to the system's IP Address.
macaddress	Sets Call Station Id Type to the system's MAC Address.
request	Configures EAP request related parameters.

retries *retries*	(Optional) For EAP messages other than Identity Requests or EAPOL (WPA) key messages, specifies the maximum number of times (0 to 20 retries) that the controller retransmits the message to a wireless client. The default value is 2.
timeout *seconds*	(Optional) For EAP messages other than Identity Requests or EAPOL (WPA) key messages, specifies the amount of time (1 to 120 seconds) that the controller waits before retransmitting the message to a wireless client. The default value is 30 seconds.
wep key	Configures 802.1x WEP related paramters.
index 0	Specifies the WEP key index value as 0
index 3	Specifies the WEP key index value as 3

Command Default

Default for eapol-key-timeout: 1 second.

Default for eapol-key-retries: 2 retries.

Command Modes

config

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1 Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

None.

This example lists all the commands under **wireless security dot1x** .

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#wireless security dot1x ?
  eapol-key         Configure eapol-key related parameters
  group-key         Configures EAP-broadcast key renew interval time in seconds
  identity-request  Configure EAP ID request related parameters
  radius            Configure radius messages
  request           Configure EAP request related parameters
  wep               Configure 802.1x WEP related paramters
  <cr>
```

wireless security dot1x radius accounting mac-delimiter

To configure a MAC delimiter for called-station-ID or a calling-station-ID, use the **wireless security dot1x radius accounting mac-delimiter** command.

To remove MAC delimiter for a called-station-ID or a calling-station-ID, use the **no** form of the command.

wireless security dot1x radius accounting mac-delimiter { **colon** | **hyphen** | **none** | **single-hyphen** }

Syntax Description

colon	Sets the delimiter to colon.
hyphen	Sets the delimiter to hyphen.
none	Disables delimiters.
single-hyphen	Sets the delimiters to single hyphen.

Command Default

None

Command Modes

Global Configuration Mode

Command History

Release	Modification
Cisco IOS XE 3.6.0 E	This command was introduced.

This example shows how to configure a MAC delimiter for called-station-ID or a calling-station-ID to colon:

```
Device(config)# wireless security dot1x radius accounting mac-delimiter colon
```

wireless security dot1x radius accounting username-delimiter

To set the delimiter type, use **wireless security dot1x radius accounting username-delimiter** command, to remove the configuration, use the **no** form of this command.

wireless security dot1x radius accounting username-delimiter {**colon | hyphen | none | single-hyphen**}

Syntax Description

colon	Sets the delimiter to colon.
hyphen	Sets the delimiter to hyphen.
none	Disables delimiters.
single-hyphen	Sets the delimiters to single hyphen.

Command Default

None

Command Modes

Global Configuration Mode.

Command History

Release	Modification
Cisco IOS XE 3.7.2 E	This command was introduced.

This example shows how to sets the delimiter to colon.

```
Device(config)# wireless security dot1x radius acounting username-delimiter colon
```

wireless security dot1x radius callStationIdCase

To configure Call Station Id CASE send in RADIUS messages, use the **wireless security dot1x radius callStationIdCase** command.

To remove the Call Station Id CASE send in RADIUS messages, use the **no** form of the command.

wireless security dot1x radius callStationIdCase {**lower** | **upper**}

Syntax Description

lower	Sends all Call Station Ids to RADIUS in lowercase
upper	Sends all Call Station Ids to RADIUS in uppercase

Command Default

None

Command Modes

Global Configuration Mode

Command History

Release	Modification
Cisco IOS XE 3.6.0 E	This command was introduced.

This example shows how to configure Call Station Id CASE send in RADIUS messages in lowercase:

```
Device(config)# wireless security dot1x radius callstationIdCase lower
```

wireless security dot1x radius mac-authentication call-station-id

To configure call station ID type for mac-authentication, use the **wireless security dot1x radius mac-authentication call-station-id** command. To remove the configuration, use the **no** form of it.

wireless security dot1x radius mac-authentication call-station-id ap-ethmac-only | ap-ethmac-ssid | ap-group-name | ap-label-address | ap-label-address-ssid | ap-location | ap-macaddress | ap-macaddress-ssid | ap-name | ap-name-ssid | ipaddress | macaddress | vlan-id

Syntax Description

ap-ethmac-only	Sets call station ID type to the AP Ethernet MAC address.
ap-ethmac-ssid	Sets call station ID type to the format 'AP Ethernet MAC address':'SSID'.
ap-group-name	Sets call station ID type to the AP Group Name.
ap-label-address	Sets call station ID type to the AP MAC address on AP Label.
ap-label-address-ssid	Sets call station ID type to the format 'AP Label MAC address': 'SSID'.
ap-location	Sets call station ID type to the AP Location.
ap-macaddress	Sets call station ID type to the AP Radio MAC Address.
ap-macaddress-ssid	Sets call station ID type to the 'AP radio MAC Address':'SSID'.
ap-name	Sets call station ID type to the AP name.
ap-name-ssid	Sets call station ID type to the format 'AP name':'SSID'.
ipaddress	Sets call station ID type to the system IP Address.
macaddress	Sets call station ID type to the system MAC Address.
vlan-id	Sets call station ID type to the VLAN ID.

Command Default

None

Command Modes

Global Configuration Mode

Command History

Release	Modification
Cisco IOS XE 3.7.2 E	This command was introduced.

The example show how to set call station ID type to the AP Ethernet MAC address:

```
Device(config)# wireless security dot1x radius mac-authentication call-station-id
ap-ethmac-only
```

wireless security dot1x radius mac-authentication mac-delimiter

To configure MAC-Authentication attributes, use the **wireless security dot1x radius mac-authentication mac-delimiter** command.

To remove MAC-Authentication attributes, use the **no** form of the command.

wireless security dot1x radius mac-authentication mac-delimiter {**colon** | **hyphen** | **none** | **single-hyphen** }

Syntax Description

colon	Sets the delimiter to colon.
hyphen	Sets the delimiter to hyphen.
none	Disables delimiters.
single-hyphen	Sets the delimiters to single hyphen.

Command Default

None

Command Modes

Global Configuration Mode

Command History

Release	Modification
Cisco IOS XE 3.6.0 E	This command was introduced.

This example shows how to configure MAC-Authentication attributes to colon:

```
Device(config)# Scurity dot1x radius mac-authentication mac-delimiter colon
```

wireless security web-auth retries

To enable web authentication retry on a particular WLAN, use the **wireless wireless security web-auth retries** command. To disable, use the **no** form of the command.

wireless securityweb-authretries*retries*
nowireless securityweb-authretries

Syntax Description

wireless security web-auth	Enables web authentication on a particular WLAN.
retries *retries*	Specifies maximum number of web authentication request retries. The range is from 0 through 30. The default value is 3.

Command Default

Command Modes

config

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1 Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

None.

This example shows how to enable web authentication retry on a particular WLAN.

```
Device#configure terminal
Device# wireless security web-auth retries 10
```

wireless tag policy

To configure wireless tag policy, use the **wireless tag policy** command.

wireless tag policy *policy-tag*

Syntax Description

policy-tag	Name of the wireless tag policy.

Command Default

The default policy tag is default-policy-tag.

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 a wireless policy tag:

```
Device(config)# wireless tag policy guest-policy
```

wireless tag site

To configure a wireless site tag, use the **wireless tag site** *site-tag*command.

wireless tag site *site-tag*

Syntax Description

site-tag	Name of 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.

Example

The following example shows how to configure a site tag:

```
Device(config)# wireless tag site test-site
```

wireless wps ap-authentication threshold

To configure the alarm trigger threshold for access point neighbor authentication, use the **wireless wps ap-authentication threshold** command. To remove the access point neighbor authentication, use the no form of the command.

wireless wps ap-authentication threshold *value*

no wireless wps ap-authentication threshold *value*

Syntax Description

threshold *value*	Specifies that the WMM-enabled clients are on the wireless LAN. The threshold value range is between 1 and 255. The default value is 1.

Command Default

None

Command Modes

Global Configuration mode

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 configure the alarm trigger threshold for access point neighbor authentication:

```
Device(config)# wireless wps ap-authentication threshold 1
```

wireless wps client-exclusion

To configure client exclusion policies, use the **wireless wps client-exclusion** command. To remove the client exclusion policies, use the **no** form of the command.

wireless wps client-exclusion {**all** | **dot11-assoc** | **dot11-auth** | **dot1x-auth** | **dot1x-timeout** | **ip-theft** | **web-auth**}
no wireless wps client-exclusion {**all** | **dot11-assoc** | **dot11-auth** | **dot1x-auth** | **dot1x-timeout** | **ip-theft** | **web-auth**}

Syntax Description

dot11-assoc	Specifies that the controller excludes clients on the sixth 802.11 association attempt, after five consecutive failures.
dot11-auth	Specifies that the controller excludes clients on the sixth 802.11 authentication attempt, after five consecutive failures.
dot1x-auth	Specifies that the controller excludes clients on the sixth 802.11X authentication attempt, after five consecutive failures.
dot1x-timeout	Enables exclusion on timeout and no response.
ip-theft	Specifies that the control excludes clients if the IP address is already assigned to another device. For more information, see the Usage Guidelines section.
web-auth	Specifies that the controller excludes clients on the fourth web authentication attempt, after three consecutive failures.
all	Specifies that the controller excludes clients for all of the above reasons.

Command Default

Enabled.

Command Modes

config

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1 Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

In IP-theft scenarios, there are differences between the older Cisco IOS XE releases and the Cisco IOS XE Denali 16.x releases:

Older Cisco IOS XE Releases	Cisco IOS XE Denali 16.x Releases
Priority wise, wired clients have higher priority over wireless clients, and DHCP IP has higher priority over static IP. The client security type is not checked; security of all client types are treated with same priority. If the existing binding is from a higher priority source, the new binding is ignored and an IP-theft is signaled. If the existing binding has the same source-priority as the new binding, the binding is ignored and an IP-theft is signaled. This ensures that the bindings are not toggled if two hosts send traffic using the same IP. Only the initial binding is retained in the software. If the new binding is from a higher priority source, the existing binding is replaced. This results in an IP-theft notification of existing binding and also a new binding notification.	There is not really a fundamental difference between wired and wireless; what matters is the trust (preflevel) of the entry, which is a function on how it was learnt (ARP, DHCP, ND, and so on) and the policy that is attached to the port. When preflevel is equal, the IP takeover is denied if the old entry is still reachable. IP takeover occurs when the update comes from a trusted port or a new entry gets IP from the DHCP server. Otherwise, you must explicitly grant it. The IP-theft is not reported if an old entry is replaced by a new and a more trusted one.

This example shows how to disable clients on the 802.11 association attempt after five consecutive failures.

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#wireless wps client-exclusion dot11-assoc
```

wireless wps mfp

To configure various Management Frame Protection (MFP) parameters, use the **wireless wps mfp** command.

wireless wps mfp **ap-impersonation** | **key-refresh-interval** *interval*

Syntax Description

interval	Specifies the MFP key refresh interval in hours. The valid range is from 1 to 24. The default value is 24.

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 configure various Management Frame Protection (MFP) parameters:

```
Device# configure terminal
Device(config)# wireless wps mfp key-refresh-interval 1
```

wireless wps mfp ap-impersonation

To configure AP impersonation detection, use the **wireless wps mfp ap-impersonation** command. Use the **no** form of this command to disable the configuration.

wireless wps mfp ap-impersonation

no wireless wps mfp ap-impersonation

Syntax Description

ap-impersonation	Configures AP impersonation detection.

Command Default

None

Command Modes

Global Configuration mode

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 configure AP impersonation detection:

```
Device(config)# wireless wps mfp ap-impersonation
```

wireless wps rogue network-assurance enable

To enable the rogue wireless service assurance (WSA) events, use the **wireless wps rogue network-assurance enable** command. Use the **no** form of this command to disable the configuration.

wireless wps rogue network-assurance enable

no wireless wps rogue network-assurance enable

Syntax Description

network-assurance enable	Enables rogue WSA events.

Command Default

None

Command Modes

Global Configuration mode

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 enable the rogue wireless service assurance events:

```
Device(config)# wireless wps rogue network-assurance enable
```

wireless wps rogue ap aaa

To configure the use of AAA/local database to detect valid AP MAC addresses, use the **wireless wps rogue ap aaa** command. Use the **no** form of this command to disable the configuration.

wireless wps rogue ap aaa

no wireless wps rogue ap aaa

Syntax Description

aaa	Configures the use of AAA or local database to detect valid AP MAC addresses.

Command Default

None

Command Modes

Global Configuration mode

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 configure the use of AAA/local database to detect valid AP MAC addresses:

```
Device(config)# wireless wps rogue ap aaa
```

wireless wps rogue ap aaa polling-interval

To configures Rogue AP AAA validation interval, in seconds, use the **wireless wps rogue ap aaa polling-interval** command. To disable the configuration, use the no form of this command.

wireless wps rogue ap aaa polling-interval *60 - 86400*

no wireless wps rogue ap aaa polling-interval *60 - 86400*

Syntax Description

aaa	Sets the use of AAA or local database to detect valid AP MAC addresses.
polling-interval	Configures the rogue AP AAA validation interval.
60 - 86400	Specifies AP AAA validation interval, in seconds.

Command Default

None

Command Modes

Global configuration

Command History

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

Usage Guidelines

None

Example

This example shows how to configures Rogue AP AAA validation interval, in seconds:

```
Device(config)# wireless wps rogue ap aaa polling-interval 120
```

wireless wps rogue ap init-timer

To configure the init timer for rogue APs, use the **wireless wps rogue ap init-timer** command. Use the **no** form of this command to disable the configuration.

wireless wps rogue ap init-timer

no wireless wps rogue ap init-timer

Syntax Description

init-timer	Configures the init timer for rogue APs.

Command Default

None

Command Modes

Global Configuration mode

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 configure the init timer for rogue APs:

```
Device(config)# wireless wps rogue ap init-timer
```

wireless wps rogue ap mac-address rldp initiate

To initiate and configure Rogue Location Discovery Protocol on rogue APs, use the **wireless wps rogue ap mac-address rldp initiate** command.

wireless wps rogue ap mac-address <*MAC Address*> **rldp initiate**

Syntax Description

wps	Configures the WPS settings.
rogue	Configures the global rogue devices.
ap mac-address <*MAC Address*>	The MAC address of the APs.
rldp initiate	Initiates RLDP on rogue APs.

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 initiate and configure Rogue Location Discovery Protocol on rogue APs:

```
Device# wireless wps rogue ap mac-address 10.1.1 rldp initiate
```

wireless wps rogue ap notify-min-rssi

To configure the minimum RSSI notification threshold for rogue APs, use the **wireless wps rogue ap notify-min-rssi** command. Use the **no** form of this command to disable the configuration.

wireless wps rogue ap notify-min-rssi

no wireless wps rogue ap notify-min-rssi

Syntax Description

notify-min-rssi	Configure the minimum RSSI notification threshold for rogue APs.

Command Default

None

Command Modes

Global Configuration mode

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 configure the minimum RSSI notification threshold for rogue APs:

```
Device(config)# wireless wps rogue ap notify-min-rssi
```

wireless wps rogue ap notify-rssi-deviation

To configure the RSSI deviation notification threshold for rogue APs, use the **wireless wps rogue ap notify-rssi-deviation** command. Use the **no** form of this command to disable the configuration.

wireless wps rogue ap notify-rssi-deviation

no wireless wps rogue ap notify-rssi-deviation

Syntax Description

notify-rssi-deviation	Configures the RSSI deviation notification threshold for rogue APs.

Command Default

None

Command Modes

Global Configuration mode

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 configure the RSSI deviation notification threshold for rogue APs:

```
Device(config)# wireless wps rogue ap notify-rssi-deviation
```

wireless wps rogue ap rldp alarm-only

To set Rogue Location Discovery Protocol (RLDP) and alarm if rogue is detected, use the **wireless wps rogue ap rldp alarm-only** command. Use the **no** form of this command to disable the configuration.

wireless wps rogue ap rldp alarm-only

no wireless wps rogue ap rldp alarm-only

Syntax Description

alarm-only	Sets RLDP and alarm if rogue is detected.

Command Default

None

Command Modes

Global Configuration mode

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 set RLDP and alarm if rogue is detected:

```
Device(config)# wireless wps rogue ap rldp alarm-only
```

wireless wps rogue ap rldp alarm-only monitor-ap-only

To perform RLDP only on monitor APs, use the **wireless wps rogue ap rldp alarm-only monitor-ap-only** command. Use the **no** form of this command to disable the configuration.

wireless wps rogue ap rldp alarm-only monitor-ap-only

no wireless wps rogue ap rldp alarm-only monitor-ap-only

Syntax Description

monitor-ap-only	Performs RLDP on monitor APs only.

Command Default

None

Command Modes

Global Configuration mode

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 perform RLDP only on monitor APs,:

```
Device(config)# wireless wps rogue ap rldp alarm-only monitor-ap-only
```

wireless wps rogue ap rldp auto-contain

To configure RLDP, alarm and auto-contain if rogue is detected, use **wirelesswps rogueaprldp auto-contain** command. Use the **no** form of the command to disable the alarm.

[no] wireless wps rogue ap rldp auto-contain monitor-ap-only

Syntax Description

monitor-ap-only	Perform RLDP only on monitor AP

Command Default

None

Command Modes

Global Configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1 Cisco IOS XE Gibraltar 16.12.1	This command was introduced.
Cisco IOS XE 3.7.3E	The **no** form of the command was introduced.

Example

This example shows how to configure an alarm for a detected rogue.

```
Device(config)#wireless wps rogue ap rldp auto-contain
```

wireless wps rogue ap rldp retries

To configure RLDP retry times on rogue APs, use the **wireless wps rogue ap rldp retries** command. Use the **no** form of this command to disable the configuration.

wireless wps rogue ap rldp retries

no wireless wps rogue ap rldp retries

Syntax Description

retries	Configures RLDP retry times on rogue APs.

Command Default

None

Command Modes

Global Configuration mode

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 configure RLDP retry times on rogue APs:

```
Device(config)# wireless wps rogue ap rldp retries
```

wireless wps rogue ap rldp schedule

To configure RLDP scheduling, use the **wireless wps rogue ap rldp schedule** command. Use the **no** form of this command to disable the configuration.

wireless wps rogue ap rldp schedule

no wireless wps rogue ap rldp schedule

Syntax Description

schedule	Configures RLDP scheduling.

Command Default

None

Command Modes

Global Configuration mode

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 configure RLDP scheduling:

```
Device(config)# wireless wps rogue ap rldp schedule
```

wireless wps rogue ap rldp schedule day

To configure the day when RLDP scheduling is to be done, use the **wireless wps rogue ap rldp schedule day** command. Use the **no** form of this command to disable the configuration.

wireless wps rogue ap rldp schedule day { **friday** | **monday** | **saturday** | **sunday** | **thursday** | **tuesday** | **wednesday** } **start** *[HH:MM:SS]* **end** *[HH:MM:SS]*

no wireless wps rogue ap rldp schedule day { **friday** | **monday** | **saturday** | **sunday** | **thursday** | **tuesday** | **wednesday** } **start** *[HH:MM:SS]* **end** *[HH:MM:SS]*

Syntax Description

day {**friday** | **monday** | **saturday** | **sunday** | **thursday** | **tuesday** | **wednesday**}	Configures the day of the week when RLDP scheduling is to be done.
start *[HH:MM:SS]*	Configures the start time for RLDP schedule for the day.
end *[HH:MM:SS]*	Configures the end time for RLDP schedule for the day.

Command Default

None

Command Modes

Global Configuration mode

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 configure the day of the week, when RLDP scheduling is to be done:

```
Device(config)# wireless wps rogue ap rldp schedule day friday start 10:10:10 end 15:15:15
```

wireless wps rogue ap timeout

To configure the expiry time for rogue APs, in seconds, use the **wireless wps rogue ap timeout** command. Use the **no** form of this command to disable the configuration.

wireless wps rogue ap timeout *240-3600*

no wireless wps rogue ap timeout *240-3600*

Syntax Description

rogue ap timeout	Configures the expiry time for rogue APs, in seconds.
240-3600	Specifies the number of seconds before rogue entries are flushed.

Command Default

None

Command Modes

Global configuration

Command History

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

Usage Guidelines

None

Example

This example shows how to configure the expiry time for rogue APs, in seconds:

```
Device(config)# wireless wps rogue ap timeout 250
```

wireless wps rogue auto-contain

To configure the auto contain level and to configure auto containment for monitor AP mode, use the **wireless wps rogue auto-contain** command. To disable the configuration, use the **no** form of this command.

wireless wps rogue auto-contain { **level** *1 - 4* | **monitor-ap-only** }

no wireless wps rogue auto-contain { **level** *1 - 4* | **monitor-ap-only** }

Syntax Description

auto-contain	Configures auto contain for rogue devices.
level	Configures auto contain levels.
1 - 4	Specifies the auto containment levels.
monitor-ap-only	Configures auto contain for monitor AP mode.

Command Default

None

Command Modes

Global configuration

Command History

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

Usage Guidelines

None

Example

This example shows how to configure the auto contain level and to configure auto containment for monitor AP mode:

```
Device(config)# wireless wps rogue auto-contain level 2
Device(config)# wireless wps rogue auto-contain monitor-ap-only
```

wireless wps rogue client aaa

To configure the use of AAA or local database to detect valid MAC addresses of rogue clients, use the **wireless wps rogue client aaa** command. Use the **no** form of this command to disable the configuration.

wireless wps rogue client aaa

no wireless wps rogue client aaa

Syntax Description

aaa	Configures the use of AAA or local database to detect valid MAC addresses of rogue clients.

Command Default

None

Command Modes

Global Configuration mode

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 configure the use of AAA or local database to detect valid MAC addresses of rogue clients:

```
Device(config)# wireless wps rogue client aaa
```

wireless wps rogue client mse

To configure Mobility Services Engine (MSE) to detect valid MAC addresses of rogue clients, use the **wireless wps rogue client mse** command. Use the **no** form of this command to disable the configuration.

wireless wps rogue client mse

no wireless wps rogue client mse

Syntax Description

mse	Configures the MSE to detect valid MAC addresses of rogue clients.

Command Default

None

Command Modes

Global Configuration mode

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 configure Mobility Services Engine (MSE) to detect valid MAC addresses of rogue clients:

```
Device(config)# wireless wps rogue client mse
```

wireless wps rogue client client-threshold

To configure rogue client per a rogue AP SNMP trap threshold, use the **wireless wps rogue client client-threshold** command. To disable the configuration, use the **no** form of this command.

wireless wps rogue client client-threshold *0 - 256*

no wireless wps rogue client client-threshold *0 - 256*

Syntax Description

rogue client	Configures rogue clients.
client-threshold	Configures the rogue client per a rogue AP SNMP trap threshold.
0 - 256	Specifies the client threshold.

Command Default

None

Command Modes

Global configuration

Command History

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

Usage Guidelines

None

Example

This example shows how to configure rogue client per a rogue AP SNMP trap threshold:

```
Device(config)# wireless wps rogue ap timeout 250
```

wireless wps rogue client notify-min-rssi

To configure the minimum RSSI notification threshold for rogue clients, use the **wireless wps rogue client notify-min-rssi** command. Use the **no** form of this command to disable the configuration.

wireless wps rogue client notify-min-rssi *-128 - -70*

no wireless wps rogue client notify-min-rssi *-128 - -70*

Syntax Description

rogue clients	Configures rogue clients.
notify-min-rssi	Configures the minimum RSSI notification threshold for rogue clients.
-128 - -70	Specifies the RSSI threshold in decibels.

Command Default

None

Command Modes

Global configuration

Command History

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

Usage Guidelines

None

Example

This example shows how to configure the minimum RSSI notification threshold for rogue clients:

```
Device(config)# wireless wps rogue client notify-min-rssi -125
```

wireless wps rogue client notify-rssi-deviation

To configure the RSSI deviation notification threshold for rogue clients, use the **wireless wps rogue client notify-rssi-deviation** command. To disable the configuration, use the **no** form of this command.

wireless wps rogue client notify-rssi-deviation *0 - 10*

no wireless wps rogue client notify-rssi-deviation *0 - 10*

Syntax Description

notify-rssi-deviation	Configures the RSSI deviation notification threshold for rogue clients.
0 - 10	Specifies the RSSI threshold in decibels.

Command Default

None

Command Modes

Global configuration

Command History

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

Usage Guidelines

None

Example

This example shows how to configure the RSSI deviation notification threshold for rogue clients:

```
Device(config)# wireless wps rogue client notify-rssi-deviation 6
```

wireless wps rogue rule

To configure rogue classification rule, use the **wireless wps rogue rule** command.

wireless wps rogue rule *rule-name* **priority** *priority* {**classify** {**friendly** | **malicious**} | **condition** {**client-count number** | **duration** | **encryption** | **infrastructure** | **rssi** | **ssid**} | **default** | **exit** | **match** {**all** | **any**} | **no** | **shutdown**}

Syntax Description

rule *rule-name*	Specifies a rule name.
priority *priority*	Changes the priority of a specific rule and shifts others in the list accordingly.
classify	Specifies the classification of a rule.
friendly	Classifies a rule as friendly.
malicious	Classifies a rule as malicious.
condition {**client-count number** | **duration** | **encryption** | **infrastructure** | **rssi** | **ssid**}	Specifies the conditions for a rule that the rogue access point must meet. Type of the condition to be configured. The condition types are listed below: • client-count—Requires that a minimum number of clients be associated to a rogue access point. The valid range is 1 to 10 (inclusive). • duration—Requires that a rogue access point be detected for a minimum period of time. The valid range is 0 to 3600 seconds (inclusive). • encryption—Requires that the advertised WLAN does not have encryption enabled. • infrastructure—Requires the SSID to be known to the controller • rssi—Requires that a rogue access point have a minimum RSSI value. The range is from –95 to –50 dBm (inclusive). • ssid—Requires that a rogue access point have a specific SSID.
default	Sets the command to its default settings.
exit	Exits the sub-mode.
match {**all** | **any**}	Configures matching criteria for a rule. Specifies whether a detected rogue access point must meet all or any of the conditions specified by the rule in order for the rule to be matched and the rogue access point to adopt the classification type of the rule.
no	Negates a command or set its defaults.
shutdown	Shuts down the system.

Command Default

None.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1Cisco IOS XE Gibraltar 16.12.1	This command was introduced.

Usage Guidelines

None.

This example shows how to create a rule that can organize and display rogue access points as Friendly:

```
Device# configure terminal
Device(config)# wireless wps rogue rule ap1 priority 1
Device(config-rule)# classify friendly
Device(config)# end
```

wireless wps rogue security-level

To configure the wireless WPS rogue detection security levels, use the **wireless wps rogue security-level** command. Use the **no** form of this command to disable the configuration.

wireless wps rogue security-level { **critical** | **custom** | **high** | **low** }

no wireless wps rogue security-level { **critical** | **custom** | **high** | **low** }

Syntax Description

rogue security-level	Configures the rogue detection security level.
critical	Specifies the rogue detection setup for highly sensitive deployments.
custom	Specifies the customizable security level.
high	Specifies the rogue detection setup for medium-scale deployments.
low	Specifies the basic rogue detection setup for small-scale deployments.

Command Default

None

Command Modes

Global configuration

Command History

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

Usage Guidelines

None

Example

This example shows how to configure the wireless WPS rogue detection security levels:

```
Device(config)# wireless wps rogue security-level critical
```

wireless-default radius server

To configure multiple radius servers, use the **wireless-default radius server** command.

wireless-default radius server *IP* **key** *secret*

Command Default None

Command Modes Global configuration (config)

Command History

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

Usage Guidelines Using this utility, you can configure a maximum of ten radius servers.

Example

This example shows how to configure multiple radius servers:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless-default radius server 9.2.58.90 key cisco123
Device(config)# end
```

wlan policy

To map a policy profile to a WLAN profile, use the **wlan policy** command.

wlan *wlan-name* **policy** *policy-name*

Syntax Description

wlan-name	Name of the WLAN profile.
policy	Map a policy profile to the WLAN profile.
policy-name	Name of the policy profile.

Command Default

None

Command Modes

config-policy-tag

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.