



Show Commands

- [show aaa dead-criteria radius](#), on page 11
- [show aaa servers](#), on page 13
- [show aaa server brief](#), on page 15
- [show access-list](#), on page 16
- [show ap name icap subscription ap rf spectrum](#), on page 18
- [show ap airtime-fairness summary](#), on page 19
- [show ap audit-report detail](#), on page 20
- [show ap audit-report summary](#), on page 21
- [show ap auth-list](#), on page 22
- [show ap auth-list ap-cert-policy](#), on page 23
- [show ap auto-rf](#), on page 24
- [show ap ble cmx detail ip](#), on page 27
- [show ap ble cmx summary](#), on page 28
- [show ap ble summary](#), on page 29
- [show ap config](#), on page 30
- [show ap config general](#), on page 31
- [show ap client-trace events all](#), on page 32
- [show ap crash-file](#), on page 33
- [show ap dot11](#), on page 34
- [show ap dot11](#), on page 40
- [show ap dot11 24ghz](#), on page 41
- [show ap dot11 24ghz SI config](#), on page 43
- [show ap dot11 24ghz SI device type](#), on page 44
- [show ap dot11 5ghz](#), on page 45
- [show ap dot11 24ghz cleanair air-quality](#), on page 47
- [show ap dot11 24ghz cleanair air-quality](#), on page 48
- [show ap dot11 cleanair config](#), on page 49
- [show ap dot11 cleanair summary](#), on page 51
- [show ap dot11 dual-band summary](#), on page 52
- [show ap environment](#), on page 53
- [show ap file-transfer https summary](#), on page 54
- [show ap filters active](#), on page 55
- [show ap filters active type priming](#), on page 56

- [show ap filters all](#), on page 57
- [show ap filters all type priming](#), on page 58
- [show ap fra](#), on page 59
- [show ap fra 5-6ghz](#), on page 60
- [show ap geolocation ranging](#), on page 61
- [show ap gps location](#), on page 62
- [show ap grpc summary](#), on page 63
- [show ap group hyperlocation](#), on page 64
- [show history channel interface dot11Radio all](#), on page 66
- [show ap hyperlocation](#), on page 67
- [show ap hyperlocation cmx summary](#), on page 69
- [show ap image](#), on page 70
- [show ap image file summary](#), on page 71
- [show ap image site summary](#), on page 73
- [show ap iot-radio firmware summary](#), on page 74
- [show ap link-encryption](#), on page 75
- [show ap lldp neighbors detail](#), on page 76
- [show ap lldp neighbors](#), on page 77
- [show ap name dot11 neighbor summary](#), on page 78
- [show ap name lldp neighbors detail](#), on page 80
- [show ap name lldp neighbors](#), on page 81
- [show ap name mesh roam history](#), on page 82
- [show ap name ntp status](#), on page 83
- [show ap ntp status](#), on page 84
- [show ap primary list](#), on page 85
- [show ap mesh cac access](#), on page 86
- [show ap mesh cac bwused voice](#), on page 87
- [show ap mesh cac callpath](#), on page 88
- [show ap mesh cac rejected](#), on page 89
- [show ap monitor-mode summary](#), on page 90
- [show ap multicast mom \(multicast over multicast\)](#), on page 91
- [show ap name *ap-name* neighbor summary](#), on page 92
- [show ap name afc detail](#), on page 94
- [show ap name afc geolocation](#), on page 95
- [show ap name afc response](#), on page 96
- [show ap name auto-rf](#), on page 97
- [show ap name ble detail](#), on page 100
- [show ap name cablemodem](#), on page 101
- [show ap name config](#), on page 102
- [show ap name config dot11 6ghz](#), on page 104
- [show ap name config slot](#), on page 105
- [show ap name config ethernet](#), on page 106
- [show ap name dot11](#), on page 107
- [show ap name dot11 6ghz power-mode](#), on page 109
- [show ap name environment](#), on page 110
- [show ap name gps location](#), on page 111

- [show ap name grpc detail](#), on page 112
- [show ap name hyperlocation](#), on page 113
- [show ap name mesh backhaul](#), on page 114
- [show ap name mesh bhrate](#), on page 115
- [show ap name mesh linktest](#), on page 116
- [show ap name mesh neighbor detail](#), on page 117
- [show ap name mesh neighbor detail](#), on page 118
- [show ap name mesh path](#), on page 119
- [show ap name mesh stats](#), on page 120
- [show ap name tunnel eogre events](#), on page 121
- [show ap name tunnel eogre domain detailed](#), on page 122
- [show ap name tunnel eogre domain summary](#), on page 123
- [show ap name tunnel eogre gateway detailed](#), on page 124
- [show ap name tunnel eogre gateway summary](#), on page 125
- [show ap name wlan](#), on page 126
- [show ap name wlan vlan](#), on page 128
- [show ap name ble detail](#), on page 129
- [show ap name temperature](#), on page 130
- [show ap management-mode meraki capability summary](#), on page 131
- [show ap management-mode meraki change summary](#), on page 132
- [show ap management-mode meraki failure summary](#), on page 133
- [show ap neighborhood](#), on page 134
- [show ap neighborhood details](#), on page 135
- [show ap neighborhood mac details](#), on page 136
- [show ap neighborhood summary](#), on page 137
- [show ap profile](#), on page 138
- [show ap rf-profile name](#), on page 139
- [show ap rf-profile summary](#), on page 141
- [show ap sensor status](#), on page 142
- [show ap summary](#), on page 143
- [show ap summary load-info](#), on page 144
- [show ap summary sort name](#), on page 145
- [show ap summary sort ascending client-count](#), on page 146
- [show ap summary sort ascending data-usage](#), on page 147
- [show ap summary sort ascending throughput](#), on page 148
- [show ap summary sort descending client-count](#), on page 149
- [show ap summary sort descending data-usage](#), on page 150
- [show ap summary sort descending throughput](#), on page 151
- [show ap support-bundle summary](#), on page 152
- [show ap tag sources](#), on page 153
- [show ap tag summary](#), on page 154
- [show ap triradio summary](#), on page 155
- [show ap timezone](#), on page 156
- [show ap upgrade](#), on page 157
- [show ap upgrade method](#), on page 158
- [show arp](#), on page 159

- [show arp summary](#) , on page 160
- [show ap tunnel eogre events](#), on page 161
- [show ap tunnel eogre domain detailed](#), on page 162
- [show ap name tunnel eogre domain summary](#), on page 163
- [show ap tunnel eogre gateway detailed](#), on page 164
- [show ap tunnel eogre gateway summary](#), on page 165
- [show ap upgrade site](#), on page 166
- [show avc client](#), on page 167
- [show avc wlan](#), on page 168
- [show awips wlc-alarm](#), on page 169
- [show awips syslog throttle](#), on page 170
- [show capwap client rcb](#), on page 171
- [show chassis](#), on page 172
- [show chassis rmi](#), on page 173
- [show checkpoint](#), on page 174
- [show cts environment data](#) , on page 181
- [show cts role-based sgt-map all](#), on page 183
- [show cts role-based counters](#), on page 185
- [show environment summary](#), on page 186
- [show etherchannel summary](#), on page 189
- [show fips authorization-key](#), on page 190
- [show fips status](#), on page 191
- [show flash wipeout-log](#), on page 192
- [show flexconnect office-extend diagnostics](#), on page 193
- [show flow exporter](#), on page 195
- [show flow interface](#), on page 197
- [show flow monitor](#), on page 199
- [show flow record](#), on page 201
- [show flow record wireless avc basic](#), on page 202
- [show flow record wireless avc ipv6 basic](#), on page 203
- [show gnxi state](#), on page 204
- [show history channel interface dot11Radio all](#), on page 206
- [show interfaces](#), on page 207
- [show interfaces dot11Radio asr-info](#), on page 211
- [show interfaces wired](#), on page 213
- [show inventory](#), on page 214
- [show ip](#), on page 216
- [show ip igmp snooping igmpv2-tracking](#), on page 217
- [show ip igmp snooping querier](#), on page 218
- [show ip igmp snooping wireless mcast-spi-count](#), on page 220
- [show ip igmp snooping wireless mgid](#), on page 221
- [show ip nbar protocol-discovery wlan](#), on page 222
- [show ipv6 access-list](#), on page 223
- [show ipv6 hop-by-hop status](#), on page 225
- [show ipv6 mld snooping](#), on page 226
- [show ipv6 mld snooping querier vlan](#), on page 228

- [show ipv6 mld snooping wireless mgid](#), on page 229
- [show ipv6 nd ra specific-route](#), on page 230
- [show ldap attributes](#), on page 231
- [show ldap server](#), on page 232
- [show license air entities](#), on page 233
- [show license all](#), on page 236
- [show license authorization](#), on page 242
- [show license data conversion](#), on page 247
- [show license eventlog](#), on page 248
- [show license history message](#), on page 249
- [show license reservation](#), on page 250
- [show license rum](#), on page 251
- [show license status](#), on page 257
- [show license summary](#), on page 267
- [show license tech](#), on page 270
- [show license udi](#), on page 285
- [show license usage](#), on page 286
- [show platform software rif-mgr chassis active R0 resource-status](#), on page 289
- [show platform software rif-mgr chassis standby R0 resource-status](#), on page 290
- [show platform software rif-mgr chassis active R0 rmi-connection-details](#), on page 291
- [show platform software rif-mgr chassis standby R0 rmi-connection-details](#), on page 292
- [show platform software rif-mgr chassis active R0 rp-connection-details](#), on page 293
- [show platform software rif-mgr chassis standby R0 rp-connection-details](#), on page 294
- [show platform software rif-mgr chassis active R0 rif-stk-internal-stats](#), on page 295
- [show platform software rif-mgr chassis standby R0 rif-stk-internal-stats](#), on page 296
- [show platform software rif-mgr chassis active R0 lmp-statistics](#), on page 297
- [show platform software rif-mgr chassis standby R0 lmp-statistics](#), on page 298
- [show platform software sl-infra](#), on page 300
- [show platform software tls client summary](#), on page 301
- [show platform software client detail](#), on page 302
- [show platform software tls statistics](#), on page 304
- [show platform software tls session summary](#), on page 306
- [show product-analytics kpi report](#), on page 307
- [show product-analytics kpi summary](#), on page 308
- [show product-analytics report detail](#), on page 309
- [show product-analytics stats](#), on page 311
- [show lisp site detail](#), on page 313
- [show logging profile wireless end timestamp](#), on page 314
- [show logging profile wireless filter](#), on page 315
- [show logging profile wireless fru](#), on page 316
- [show logging profile wireless internal](#), on page 317
- [show logging profile wireless level](#), on page 318
- [show logging profile wireless module](#), on page 319
- [show logging profile wireless reverse](#), on page 320
- [show logging profile wireless start](#), on page 321
- [show logging profile wireless switch](#), on page 322

- [show logging profile wireless to-file](#), on page 323
- [show mdns-sd cache](#), on page 324
- [show mdns-sd cache detail](#), on page 325
- [show mdns-sd cache upn shared](#), on page 326
- [show mdns-sd cache upn detail](#), on page 328
- [show mdns-sd flexconnect summary](#), on page 329
- [show mdns-sd statistics](#), on page 330
- [show mdns-sd summary](#), on page 331
- [show mdns-sd sp-sdg statistics](#), on page 332
- [show mobility](#), on page 333
- [show monitor capture](#), on page 335
- [show nmsp](#), on page 338
- [show nmsp cloud-services statistics](#), on page 339
- [show nmsp cloud-services summary](#), on page 340
- [show nmsp subscription group detail all](#), on page 341
- [show nmsp subscription group detail ap-list](#), on page 342
- [show nmsp subscription group detail services](#), on page 343
- [show nmsp subscription group summary](#), on page 344
- [show ntp associations](#), on page 345
- [show parameter-map type webauth name](#), on page 346
- [show platform conditions](#), on page 347
- [show platform hardware](#), on page 348
- [show platform hardware chassis active qfp feature dns-snoop-agent client enabled-intf](#), on page 349
- [show platform hardware chassis active qfp feature dns-snoop-agent client hw-pattern-list](#), on page 350
- [show platform hardware chassis active qfp feature dns-snoop-agent client info](#), on page 351
- [show platform hardware chassis active qfp feature dns-snoop-agent client pattern-list](#), on page 352
- [show platform hardware chassis active qfp feature dns-snoop-agent datapath ip-cache](#), on page 353
- [show platform hardware chassis active qfp feature dns-snoop-agent datapath memory](#), on page 354
- [show platform hardware chassis active qfp feature dns-snoop-agent datapath regexp-table](#), on page 355
- [show platform hardware chassis active qfp feature dns-snoop-agent datapath stats](#), on page 356
- [show platform hardware chassis active qfp feature et-analytics datapath runtime](#), on page 357
- [show platform hardware chassis active qfp feature et-analytics datapath memory](#), on page 358
- [show platform hardware chassis active qfp feature et-analytics datapath stats export](#), on page 359
- [show platform hardware chassis active qfp feature et-analytics datapath stats flow](#), on page 360
- [show platform hardware chassis active qfp feature wireless et-analytics eta-pending-client-tree](#), on page 361
- [show platform hardware chassis active qfp feature wireless et-analytics statistics](#), on page 362
- [show platform hardware slot R0 ha_port interface stats](#), on page 363
- [show platform integrity](#), on page 366
- [show platform software audit](#), on page 367
- [show platform software arp broadcast](#), on page 369
- [show platform software system all](#), on page 370
- [show platform software trace filter-binary](#), on page 371
- [show platform software trace filter-binary](#), on page 372
- [show platform software trace level](#), on page 373
- [show platform software utd chassis active F0 et-analytics global](#), on page 376

- show platform software et-analytics global, on page 377
- show platform sudi certificate, on page 378
- show platform sudi pki, on page 380
- show parameter-map type umbrella global, on page 381
- show policy-map, on page 382
- show processes cpu, on page 387
- show rate-limit client, on page 389
- show remote-lan all, on page 390
- show remote-lan id, on page 391
- show remote-lan name, on page 392
- show remote-lan policy detail, on page 393
- show remote-lan policy summary, on page 395
- show remote-lan summary, on page 396
- show sdavc ap download status, on page 397
- show sdavc status ap, on page 398
- show ssh , on page 399
- show split-tunnel client access-list, on page 400
- show tech-support wireless, on page 401
- show tech-support wireless ap, on page 403
- show tech-support wireless client, on page 413
- **show tech-support wireless datapath**, on page 417
- show tech-support wireless fabric, on page 438
- **show tech-support wireless mobility**, on page 439
- show tech-support wireless radio, on page 451
- show tunnel eogre global-configuration, on page 462
- show tunnel eogre domain detailed, on page 463
- show tunnel eogre domain summary, on page 464
- show tunnel eogre gateway summary, on page 465
- show tunnel eogre gateway detailed , on page 466
- show tunnel eogre manager stats global, on page 467
- show tunnel eogre manager stats instance, on page 469
- show umbrella config, on page 471
- show umbrella deviceid, on page 472
- show umbrella deviceid detailed, on page 473
- show umbrella dnscrypt, on page 474
- show vlan, on page 475
- show vlan access-map, on page 478
- show vlan filter, on page 479
- show vlan group, on page 480
- show vrrp events, on page 481
- show vrrp statistics, on page 482
- show vrrp status, on page 483
- show wireless afc ap, on page 484
- show wireless afc channels , on page 485
- show wireless afc geolocation, on page 486
- show wireless afc request, on page 487

- [show wireless afc response](#), on page 488
- [show wireless afc statistics](#), on page 489
- [show wireless stats ap history](#), on page 490
- [show wireless stats ap join summary](#), on page 491
- [show wireless stats ap join summary sort](#), on page 492
- [show wireless stat redundancy statistics client-recovery mobilityd](#) , on page 493
- [show wireless stat redundancy statistics client-recovery sisf](#), on page 494
- [show wireless stat redundancy client-recovery wncd](#), on page 495
- [show wireless band-select](#), on page 496
- [show wireless certification config](#), on page 497
- [show wireless client](#) , on page 498
- [show wireless client mac-address](#) , on page 499
- [show wireless client mac-address \(Call Control\)](#), on page 501
- [show wireless client mac-address \(TCLAS\)](#), on page 502
- [show wireless client mac-address mobility history](#), on page 503
- [show wireless client mac-address stats latency](#) , on page 504
- [show wireless client summary](#), on page 505
- [show wireless client timers](#), on page 506
- [show wireless country](#), on page 507
- [show wireless detail](#), on page 510
- [show wireless dhcp relay statistics](#), on page 511
- [show wireless dot11h](#) , on page 512
- [show wireless dtls connections](#), on page 513
- [show wireless exclusionlist](#) , on page 514
- [show wireless exclusionlist client mac-address detail](#), on page 515
- [show wireless fabric summary](#), on page 517
- [show wireless fabric client summary](#) , on page 518
- [show wireless fabric vnid mapping](#), on page 519
- [show wireless flow-control](#), on page 520
- [show wireless flow-control statistics](#), on page 521
- [show wireless load-balancing](#), on page 522
- [show wireless mesh ap fabric summary](#), on page 523
- [show wireless media-stream client detail](#) , on page 524
- [show wireless media-stream group](#), on page 525
- [show wireless media-stream message details](#) , on page 526
- [show wireless mobility controller ap](#), on page 527
- [show wireless media-stream multicast-direct state](#) , on page 528
- [show wireless mesh ap](#) , on page 529
- [show wireless mesh ap summary](#) , on page 530
- [show wireless mesh ap tree](#), on page 531
- [show wireless mesh ap tree](#), on page 532
- [show wireless mesh cac summary](#), on page 533
- [show wireless mesh config](#) , on page 534
- [show wireless mesh rrm dca status](#), on page 535
- [show wireless mesh neighbor](#) , on page 536
- [show wireless profile ap priming summary](#), on page 538

- [show wireless mobility](#), on page 539
- [show wireless mobility peer ip](#) , on page 540
- [show wireless multicast group summary](#) , on page 541
- [show wireless mobility summary](#) , on page 542
- [show wireless multicast](#), on page 543
- [show wireless multicast group](#), on page 544
- [show wireless mesh ethernet daisy-chain summary](#), on page 545
- [show wireless mesh ethernet daisy-chain bgn](#), on page 546
- [show wireless performance](#), on page 547
- [show wireless pmk-cache](#), on page 548
- [show wireless probe](#), on page 549
- [show wireless profile ap priming all](#), on page 550
- [show wireless profile ap priming all](#), on page 551
- [show wireless profile airtime-fairness mapping](#), on page 552
- [show wireless profile airtime-fairness summary](#), on page 553
- [show wireless profile ap packet-capture](#), on page 554
- [show wireless profile calendar-profile detailed](#), on page 556
- [show wireless profile calendar-profile summary](#), on page 557
- [show wireless profile fabric detailed](#), on page 558
- [show wireless profile flex](#) , on page 559
- [show wireless profile policy all](#), on page 560
- [show wireless profile policy detailed](#) , on page 561
- [show wireless profile mesh detailed](#), on page 562
- [show wireless profile radio summary](#), on page 563
- [show wireless profile tunnel summary](#), on page 564
- [show wireless redundancy statistics](#) , on page 565
- [show wireless rfid](#), on page 566
- [show wireless stats ap name](#), on page 567
- [show wireless stats ap image-download](#), on page 569
- [show wireless stats client delete reasons](#), on page 570
- [show wireless statistics mobility](#) , on page 576
- [show wireless stats mesh packet error](#) , on page 577
- [show wireless stats pmk-propagation](#) , on page 578
- [show wireless stats mesh security and queue](#), on page 579
- [show wireless stats client detail](#), on page 580
- [show wireless stats redundancy config database](#), on page 581
- [show wireless summary](#), on page 582
- [show wireless tag rf](#), on page 583
- [show wireless urlfilter details](#), on page 584
- [show wireless urlfilter summary](#), on page 585
- [show wireless vlan details](#) , on page 586
- [show wireless wgb mac-address](#) , on page 587
- [show wireless wgb summary](#) , on page 588
- [show wireless wps mfp ap summary](#), on page 589
- [show wireless wps mfp statistics](#), on page 590
- [show wireless wps mfp summary](#), on page 591

- [show wireless wps rogue](#) , on page 592
- [show wireless wps rogue ap summary](#) , on page 593
- [show wireless wps rogue client detailed](#), on page 594
- [show wireless wps rogue ap detailed](#), on page 595
- [show wireless wps rogue client summary](#), on page 596
- [show wireless wps summary](#), on page 597
- [show wlan name client stats](#), on page 598
- [show wlan summary sort ascending client-count](#), on page 599
- [show wlan summary sort descending client-count](#), on page 600
- [show wlan summary sort ascending data-usage](#), on page 601
- [show wlan summary sort descending data-usage](#), on page 602
- [show wps summary](#), on page 603
- [shutdown](#), on page 604

show aaa dead-criteria radius

To verify the dead-server-detection information for a RADIUS server, use the **show aaa dead-criteria radius** command.

show aaa dead-criteria radius *ipaddr* **auth-port** *authport* **acct-port** *acctport*

| Syntax Description | <i>ipaddr</i> IP address. | | | | |
|--------------------------------|---|---------|--------------|--------------------------------|---|
| | <i>authport</i> Authentication port. | | | | |
| | <i>acctport</i> Accounting port. | | | | |
| Command Default | None | | | | |
| Command Modes | Privileged EXEC (#) | | | | |
| Command History | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.10.1</td> <td>This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td> </tr> </tbody> </table> | 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. |
| 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 show aaa dead-criteria radius <i>ipaddr</i> command displays output only if default ports are used. For non-default ports, use the show aaa dead-criteria radius <i>ipaddr</i> auth-port <i>authport</i> acct-port <i>acctport</i> command. | | | | |

Example

The following example shows how to see the dead-server-detection information for a RADIUS server with non-default authorization and accounting ports:

```
Device# show aaa dead-criteria radius 4.4.4.4 auth-port 4444 acct-port 3333
```

```
RADIUS: No server group specified. Using radius
RADIUS Server Dead Criteria:
=====
Server Details:
Address : 4.4.4.4
Auth Port : 4444
Acct Port : 3333
Server Group : radius
Dead Criteria Details:
Configured Retransmits : 3
Configured Timeout : 5
Estimated Outstanding Access Transactions: 0
Estimated Outstanding Accounting Transactions: 0
Dead Detect Time : 10s
Computed Retransmit Tries: 10
Statistics Gathered Since Last Successful Transaction
=====
Max Computed Outstanding Transactions: 0
Max Computed Dead Detect Time: 0s
```

```
Max Computed Retransmits : 0
```

The following example shows how to see the dead-server-detection information for a RADIUS server using default ports:

```
Device# show aaa dead-criteria radius 9.3.13.37

RADIUS: No server group specified. Using radius
RADIUS Server Dead Criteria:
=====
Server Details:
Address : 9.3.13.37
Auth Port : 1812
Acct Port : 1813
Server Group : radius
Dead Criteria Details:
Configured Retransmits : 3
Configured Timeout : 30
Estimated Outstanding Access Transactions: 1
Estimated Outstanding Accounting Transactions: 0
Dead Detect Time : 10s
Computed Retransmit Tries: 10
Statistics Gathered Since Last Successful Transaction
=====
Max Computed Outstanding Transactions: 4
Max Computed Dead Detect Time: 48s
Max Computed Retransmits : 30
```

show aaa servers

To display the status and number of packets that are sent to and received from all public and private authentication, authorization, and accounting (AAA) RADIUS servers as interpreted by the AAA Server MIB, use the **show aaa servers** command.

show aaa servers [private | public]

| Syntax Description | <p>private (Optional) Displays private AAA servers only, which are also displayed by the AAA Server MIB.</p> <p>public (Optional) Displays public AAA servers only, which are also displayed by the AAA Server MIB.</p> | | | | |
|--------------------------------|---|---------|--------------|--------------------------------|---|
| Command Default | None | | | | |
| Command Modes | Privileged EXEC(#) | | | | |
| Command History | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.10.1</td> <td>This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td> </tr> </tbody> </table> | 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. |
| 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 | Only RADIUS servers are supported by the show aaa servers command. | | | | |

Example

The following command displays information about packets sent and received for all AAA transaction types--authentication, authorization, and accounting.

```
Device# show aaa servers

RADIUS: id 2, priority 1, host 124.2.2.12, auth-port 1645, acct-port 1612, hostname rsim
  State: current UP, duration 20699s, previous duration 0s
  Dead: total time 0s, count 0
  Platform State from SMD: current UP, duration 20699s, previous duration 0s
  SMD Platform Dead: total time 0s, count 0
  Platform State from WNCDC (1) : current UP
  Platform State from WNCDC (2) : current UP
  Platform State from WNCDC (3) : current UP
  Platform State from WNCDC (4) : current UP
  Platform State from WNCDC (5) : current UP
  Platform State from WNCDC (6) : current UP
  Platform State from WNCDC (7) : current UP
  Platform State from WNCDC (8) : current UP, duration 964s, previous duration 0s
  Platform Dead: total time 0s, count 0UP
  Quarantined: No
.
.
.

Elapsed time since counters last cleared: 5h44m
Estimated Outstanding Access Transactions: 0
Estimated Outstanding Accounting Transactions: 0
Estimated Throttled Access Transactions: 0
Estimated Throttled Accounting Transactions: 0
```

```
Maximum Throttled Transactions: access 0, accounting 0
Consecutive Response Failures: total 0
    SMD Platform : max 0, current 0 total 0
    WNCN Platform: max 0, current 0 total 0
    IOSD Platform : max 0, current 0 total 0
Consecutive Timeouts: total 0
    SMD Platform : max 0, current 0 total 0
    WNCN Platform: max 0, current 0 total 0
    IOSD Platform : max 0, current 0 total 0
Requests per minute past 24 hours:
    high - 5 hours, 44 minutes ago: 0
    low  - 5 hours, 44 minutes ago: 0
    average: 0
```

show aaa server brief

To view the summary information of Authentication, Authorization, and Accounting (AAA) servers, use the **show aaa server brief** command.

show aaa server brief

| | |
|---------------------------|--|
| Syntax Description | This command has no keywords or arguments. |
|---------------------------|--|

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

| | |
|----------------------|---------------------|
| Command Modes | Privileged EXEC (#) |
|----------------------|---------------------|

| | | |
|------------------------|-----------------------------|------------------------------|
| Command History | Release | Modification |
| | Cisco IOS XE Dublin 17.11.1 | This command was introduced. |

Examples

The following example shows how to view the summary information of AAA servers:

```
Device# show aaa server brief
```

| Access Reqs | Access Total Requests (Auth+Acct) | Access Resp Accept (IOSD) | Access Uptime Reject (SMD) | Access Uptime timeouts (WNCD) | Outstndg Acct. tx | Acct. Req | Acct. Responses | Outstndg timeouts | Total Acct. |
|------------------|-----------------------------------|---------------------------|----------------------------|-------------------------------|-------------------|-----------|-----------------|-------------------|-------------|
| rsim | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | | 2372790 | 2372790 | 964 | | | | |
| R1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | | 2372790 | 2372790 | 964 | | | | |
| free-radius-auth | | | | | | | | | |
| hc-server | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | | 2372790 | 2372790 | 964 | | | | |
| cisco-dnac-auth | | | | | | | | | |
| z-server | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | | 2372790 | 2372790 | 964 | | | | |
| r1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | | 2372790 | 2372790 | 964 | | | | |
| ise | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | | 2372790 | 2372790 | 964 | | | | |
| Radius-2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | | 2274176 | 2274176 | 296805 | | | | |

show access-list

To display access control lists (ACLs) configured on the device, use the **show access-lists** command in privileged EXEC mode.

show access-lists[{*namenumber* | **hardware counters** | **ipc**}]

| Syntax Description | |
|--------------------------|---|
| <i>number</i> | (Optional) ACL number. The range is 1 to 2799. |
| <i>name</i> | (Optional) Name of the ACL. |
| hardware counters | (Optional) Displays the access list hardware counters. |
| ipc | (Optional) Display Interprocess Communication (IPC) protocol access-list configuration download information |

Command Default

Privileged EXEC

Command History

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

Usage Guidelines

Though visible in the command-line help strings, the **rate-limit** keyword is not supported

The device supports only IP standard and extended access lists. Therefore, the allowed numbers are only 1 to 199 and 1300 to 2799.

This command also displays the MAC ACLs that are configured.

This is an example of output from the **show access-lists** command:

```
Device# show access-lists

Extended IP access list 103
  10 permit ip any any dscp af11
Extended IP access list ssm-range
  10 deny ip any 232.0.0.0 0.255.255.255
  20 permit ip any any
Extended MAC access list macl
```

This is an example of output from the **show access-lists hardware counters** command:

```
Device# show access-lists hardware counters
L3 ACL INPUT Statistics
  All Drop:                               frame count: 0
  All Bridge Only:                         frame count: 0
  All Forwarding To CPU:                   frame count: 294674
  All Forwarded:                           frame count: 2577677
```



```
All Drop And Log:          frame count: 0
All Bridge Only And Log:   frame count: 0
All Forwarded And Log:    frame count: 0
All IPv6 Drop:            frame count: 0
All IPv6 Bridge Only:     frame count: 0
All IPv6 Forwarding To CPU: frame count: 0
All IPv6 Forwarded:       frame count: 102
All IPv6 Drop And Log:    frame count: 0
All IPv6 Bridge Only And Log: frame count: 0
All IPv6 Forwarded And Log: frame count: 0
```

L3 ACL OUTPUT Statistics

```
All Drop:                  frame count: 0
All Bridge Only:          frame count: 0
All Forwarding To CPU:    frame count: 0
All Forwarded:            frame count: 266050
All Drop And Log:        frame count: 0
All Bridge Only And Log:  frame count: 0
All Forwarded And Log:    frame count: 0
All IPv6 Drop:           frame count: 0
All IPv6 Bridge Only:    frame count: 0
All IPv6 Forwarding To CPU: frame count: 0
All IPv6 Forwarded:      frame count: 0
All IPv6 Drop And Log:   frame count: 0
All IPv6 Bridge Only And Log: frame count: 0
All IPv6 Forwarded And Log: frame count: 0
```

show ap name icap subscription ap rf spectrum

To display the spectrum configuration details of a corresponding AP, use the **show ap name icap subscription ap rf spectrum** command.

show ap name *ap_name* **icap subscription ap rf spectrum**

| Syntax Description | <i>ap_name</i> AP name | | | | |
|-------------------------------|---|---------|--------------|-------------------------------|------------------------------|
| Command Default | None | | | | |
| Command Modes | Privileged EXEC (#) | | | | |
| Command History | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 17.2.1</td> <td>This command was introduced.</td> </tr> </tbody> </table> | Release | Modification | Cisco IOS XE Gibraltar 17.2.1 | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE Gibraltar 17.2.1 | This command was introduced. | | | | |

Example

The following example shows how to display spectrum analysis on a AP:

```
Device# show ap name 4800AP icap subscription ap rf spectrum
Per-AP ICap configuration

AP RF spectrum subscription
  State           : enabled
  Radio slots     : none
```

show ap airtime-fairness summary

To view the ATF configuration summary of all radios, use the **show ap airtime-fairness summary** command.

```
show ap airtime-fairness summary
```

Syntax Description

This command has no arguments.

Command Default

None

Command Modes

Global configuration

Command History

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

This example shows how to view the ATF configuration summary of all radios:

```
Device# show ap airtime-fairness summary
```

show ap audit-report detail

To display the configuration of an AP, use the **show ap *ap-name* audit-report detail** command.

show ap *ap-name* audit-report detail

| | | |
|---------------------------|-------------------------------|----------------------------------|
| Syntax Description | <i>ap-name</i> | AP name. |
| | detail | Displays audit report for an AP. |
| Command Default | None | |
| Command Modes | Privileged EXEC (#) | |
| Command History | Release | Modification |
| | Cisco IOS XE Amsterdam 17.3.1 | This command was introduced. |

Example

This following example shows how to display the audit report for an AP:

```
Device# show ap Cisco-AP audit-report detail
```

```
Cisco AP Name : Cisco-AP
```

```
=====
```

```
Radio Audit Report:
```

| Slot | Channel | Bandwidth | Tx Power | Admin State | Operation State | Radio Role |
|-----------------|---------|-----------|----------|-------------|-----------------|------------|
| Radio Operation | | | | | | |
| 0 | IN_SYNC | IN_SYNC | IN_SYNC | OUT_OF_SYNC | IN_SYNC | IN_SYNC |
| 1 | IN_SYNC | IN_SYNC | IN_SYNC | OUT_OF_SYNC | IN_SYNC | IN_SYNC |

```
WLAN Audit Report:
```

| Slot-id | Wlan-id | Vlan | State | SSID | Auth Type | Flags |
|---------|---------|------|---------|-------------|-----------|---------|
| 0 | 1 | | IN_SYNC | OUT_OF_SYNC | IN_SYNC | IN_SYNC |
| 0 | 2 | | IN_SYNC | OUT_OF_SYNC | IN_SYNC | IN_SYNC |
| 1 | 1 | | IN_SYNC | OUT_OF_SYNC | IN_SYNC | IN_SYNC |
| 1 | 2 | | IN_SYNC | OUT_OF_SYNC | IN_SYNC | IN_SYNC |

show ap audit-report summary

To display the audit report summary for an AP, use the **show ap audit-report summary** command.

show ap audit-report summary

| | |
|---------------------------|--------------------------------|
| Syntax Description | This command has no arguments. |
|---------------------------|--------------------------------|

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

| | |
|----------------------|---------------------|
| Command Modes | Privileged EXEC (#) |
|----------------------|---------------------|

| Command History | Release | Modification |
|------------------------|-------------------------------|------------------------------|
| | Cisco IOS XE Amsterdam 17.3.1 | This command was introduced. |

Example

The following example shows how to display the audit report summary of an AP:

```
Device# show ap audit-report summary
WTP Mac           Radio           Wlan           IPv4 Acl
IPv6 Acl          Last Report Time
-----
1880.90fd.6b40    OUT_OF_SYNC     OUT_OF_SYNC     IN_SYNC         IN_SYNC         01/01/1970
05:30:00 IST
```

show ap auth-list

To see the access point authorization list, use the **show ap auth-list** command.

show ap auth-list [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

Syntax Description

| | |
|-----------------------|---|
| <i>chassis-number</i> | Chassis number as either 1 or 2. |
| active R0 | Active instance in Route-processor slot 0. |
| standby R0 | Standby instance in Route-processor slot 0. |

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Examples

The following example shows how to see the access point authorization list:

```
Device# show ap auth-list
```

show ap auth-list ap-cert-policy

To verify if the APs have been authorized by the AP certificate policy, use the **show ap auth-list ap-cert-policy**

show ap auth-list ap-cert-policy

| | |
|---------------------------|--------------------------------|
| Syntax Description | This command has no arguments. |
|---------------------------|--------------------------------|

| | |
|------------------------|---------------------|
| Command Default | Privileged EXEC (#) |
|------------------------|---------------------|

| Command History | Release | Modification |
|------------------------|-------------------------------|------------------------------|
| | Cisco IOS XE Bengaluru 17.5.1 | This command was introduced. |

Example

The following example shows how to verify if the APs have been authorized by the AP certificate policy:

```
Device# show ap auth-list ap-cert-policy
```

show ap auto-rf

To display the auto-RF settings for a Cisco lightweight access point, use the **show ap auto-rf** command.

```
show ap auto-rf dot11 {24ghz | 5ghz | dual-band} cisco_ap
```

| Syntax Description | | |
|--------------------|------------------|---------------------------|
| | 24ghz | Specifies the 802.11b AP. |
| | 5ghz | Specifies the 802.11a AP. |
| | dual-band | Specifies dual bands. |

Command Default None

Usage Guidelines The **show ap auto-rf** command output will not display neighbor AP names.

The following example shows how to display auto-RF information for an access point:

```
Device# show ap auto-rf dot11 24ghz AP1

#####

Number of Slots                : 3
AP Name                        : APA023.9FD8.EA22
MAC Address                    : 40ce.24bf.8ca0
Ethernet MAC Address          : a023.9fd8.ea22
  Slot ID                      : 0
  Radio Type                   : 802.11n - 2.4 GHz
  Current TX/RX Band           : 2.4Ghz band
  Subband Type                 : All
Noise Information
  Noise Profile                : Passed
  Channel 1                    : -91 dBm
  Channel 2                    : -67 dBm
  Channel 3                    : -54 dBm
  Channel 4                    : -55 dBm
  Channel 5                    : -71 dBm
  Channel 6                    : -85 dBm
  Channel 7                    : -50 dBm
  Channel 8                    : -54 dBm
  Channel 9                    : -77 dBm
  Channel 10                   : -88 dBm
  Channel 11                   : -65 dBm
Interference Information
  Interference Profile         : Failed
  Channel 1                    : -47 dBm @ 21% busy
  Channel 2                    : -45 dBm @ 2% busy
  Channel 3                    : -128 dBm @ 0% busy
  Channel 4                    : -128 dBm @ 0% busy
  Channel 5                    : -48 dBm @ 2% busy
  Channel 6                    : -45 dBm @ 2% busy
  Channel 7                    : -42 dBm @ 3% busy
  Channel 8                    : -128 dBm @ 0% busy
  Channel 9                    : -128 dBm @ 0% busy
  Channel 10                   : -39 dBm @ 3% busy
  Channel 11                   : -46 dBm @ 3% busy
Rogue Histogram (20)
  Channel 1                    : 36
```



```

Channel 2 : 0
Channel 3 : 0
Channel 4 : 1
Channel 5 : 0
Channel 6 : 11
Channel 7 : 0
Channel 8 : 1
Channel 9 : 3
Channel 10 : 0
Channel 11 : 14
Load Information
Load Profile : Failed
Receive Utilization : 0%
Transmit Utilization : 0%
Channel Utilization : 98%
Attached Clients : 0 clients
Coverage Information
Coverage Profile : Passed
Failed Clients : 0 clients
Client Signal Strengths
RSSI -100 dBm : 0 clients
RSSI -92 dBm : 0 clients
RSSI -84 dBm : 0 clients
RSSI -76 dBm : 0 clients
RSSI -68 dBm : 0 clients
RSSI -60 dBm : 0 clients
RSSI -52 dBm : 0 clients
Client Signal to Noise Ratios
SNR 0 dB : 0 clients
SNR 5 dB : 0 clients
SNR 10 dB : 0 clients
SNR 15 dB : 0 clients
SNR 20 dB : 0 clients
SNR 25 dB : 0 clients
SNR 30 dB : 0 clients
SNR 35 dB : 0 clients
SNR 40 dB : 0 clients
SNR 45 dB : 0 clients
Nearby APs
AP d0ec.3572.b9a0 slot 0 : -23 dBm on ( 11, 20 MHz) (181.22.0.22)
AP 0c75.bdb3.9000 slot 0 : -28 dBm on ( 11, 20 MHz) (181.21.0.21)
AP a4b2.3980.3740 slot 0 : -28 dBm on ( 1, 20 MHz) (181.21.0.21)
AP d0ec.3576.8320 slot 0 : -33 dBm on ( 11, 20 MHz) (50.1.1.122)
AP a0f8.49dc.9780 slot 0 : -34 dBm on ( 1, 20 MHz) (9.9.57.94)
AP a0f8.49dc.8260 slot 0 : -34 dBm on ( 6, 20 MHz) (9.9.57.94)
AP d0ec.3573.7c80 slot 0 : -36 dBm on ( 6, 20 MHz) (192.185.183.44)

AP 00b0.e192.9d20 slot 0 : -36 dBm on ( 11, 20 MHz) (9.9.42.47)
AP a4b2.397f.41c0 slot 0 : -36 dBm on ( 1, 20 MHz) (185.10.0.10)
AP 2c5a.0fd5.b8c0 slot 0 : -36 dBm on ( 6, 20 MHz) (9.7.97.51)
AP a488.7351.4740 slot 0 : -36 dBm on ( 11, 20 MHz) (9.7.97.51)
AP 10b3.d5e9.c8e0 slot 0 : -36 dBm on ( 1, 20 MHz) (50.1.1.122)
AP 0c75.bdb3.ab00 slot 0 : -37 dBm on ( 6, 20 MHz) (185.10.0.10)
AP 68ca.e451.5120 slot 0 : -37 dBm on ( 1, 20 MHz) (9.4.155.15)
AP a0f8.49dc.97a0 slot 0 : -37 dBm on ( 11, 20 MHz) (9.9.57.94)
AP 188b.4501.7940 slot 0 : -38 dBm on ( 11, 20 MHz) (9.9.57.94)
AP 002c.c88a.f8e0 slot 0 : -38 dBm on ( 11, 20 MHz) (9.9.50.55)
AP 7069.5a78.4960 slot 0 : -38 dBm on ( 11, 20 MHz) (9.7.97.51)
AP 3c41.0ea7.0880 slot 0 : -39 dBm on ( 11, 20 MHz) (185.10.0.10)
AP a0f8.49dc.93a0 slot 0 : -39 dBm on ( 6, 20 MHz) (9.9.57.94)
AP f4db.e685.7360 slot 0 : -39 dBm on ( 6, 20 MHz) (50.1.1.122)
AP 7070.8bb4.4120 slot 0 : -40 dBm on ( 11, 20 MHz) (9.9.57.94)
AP 707d.b93e.39e0 slot 0 : -40 dBm on ( 1, 20 MHz) (4.4.4.1)
AP 706d.150c.6860 slot 0 : -40 dBm on ( 11, 20 MHz) (50.1.1.122)

```

```

Radar Information
Channel Assignment Information via DCA
  Current Channel Average Energy      : -50 dBm
  Previous Channel Average Energy     : -50 dBm
  Channel Change Count                : 9
  Last Channel Change Time            : 02/14/2021 20:54:57
  Recommended Best Channel            : 1
RF Parameter Recommendations
  Power Level                         : 8
  RTS/CTS Threshold                   : 2347
  Fragmentation Threshold              : 2346
  Antenna Pattern                     : 0
Persistent Interference Devices
Class Type      Channel  DC (%)  RSSI (dBm)  Last Update Time
-----
All third party trademarks are the property of their respective owners.

```

show ap ble cmx detail ip

To view the BLE management feature related global values for a specific CMX along with all the APs associated to that CMX, use the **show ap ble cmx detail ip** command.

show ap ble cmx detail ip *CMX-IP*

Syntax Description

CMX-IP Specifies the IPv4 address.

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

This example shows how to display the BLE management feature related global values for a specific CMX along with all the APs associated to that CMX:

```
Device# show ap ble cmx detail ip 10.1.2.3
BLE administrative status: Up
BLE operational status: Up
Scanning interval: 10
```

| AP Name | Interface | Status |
|------------------|------------|--------|
| AP4001.7AB2.C39A | Integrated | Open |

show ap ble cmx summary

To view the list of all CMXs registered for BLE Management feature and their global values for BLE, use the **show ap ble cmx summary** command.

show ap ble cmx summary

| | |
|---------------------------|--|
| Syntax Description | This command has no keywords or arguments. |
|---------------------------|--|

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

| | |
|----------------------|-----------------|
| Command Modes | Privileged EXEC |
|----------------------|-----------------|

| Command History | Release | Modification |
|------------------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.11.1 | This command was introduced. |

Usage Guidelines

This example shows how to view the list of all CMXs registered for BLE Management feature and their global values for BLE:

```
Device# show ap ble cmx summary
CMX IP: 10.1.2.3
-----
BLE administrative status: Up
BLE operational status: Up
Scanning interval: 12

CMX IP: 10.1.2.4
-----
BLE administrative status: Down
BLE operational status: Down
Reason: BLE is administratively down
Scanning interval: 0

CMX IP: 10.1.2.5
-----
BLE administrative status: Up
BLE operational status: Down
Reason: CMX is not subscribed to AP Monitor and RSSI services, or NMSP connection is down
Scanning interval: 10
```

show ap ble summary

To view the list of joined APs that support BLE Management feature along with the BLE details for each AP, use the **show ap ble summary** command.

show ap ble summary

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|--------------------------------|--|
| | Cisco IOS XE Gibraltar 16.11.1 | This command was introduced. |
| | Cisco IOS XE Cupertino 17.9.1 | The output of the command is modified to add new column that displays scan status. |

Usage Guidelines The BLE Management feature is enabled and APs are displayed only when the CMX is registered with the controller, and BLE is enabled on CMX.

This example shows how to view the list of joined APs that support BLE Management feature along with the BLE details for each AP:

```

Device# show ap ble summary
AP Name                               Interface           Status             CMX IP
-----
AP4001.7AB2.C39A                      Integrated          Open               10.1.2.3
AP4001.7AB2.C39B                      Integrated          Closed             10.1.2.4

Device# show ap ble summary
AP Name  AP Model  AP Ethernet MAC  BLE           BLE           BLE mode  BLE
MAC      BLE Profile  BLE Scan        Interface State  Admin State
-----
AP794   C9130AXI-B  04eb.409e.xxxx  Open          Up            Base (Native)
806f.b031.xxxx  Eddystone URL  Enabled/Disabled
AP50    C9130AXI-B  04eb.409e.xxxx  Close         Down          Base (Native)
Unknown Not Configured Enabled/Disabled
AP28    C9136I     687d.b45c.xxxx  Close         Down          Base (Native)
Unknown Not Configured Enabled/Disabled
    
```

show ap config

To display configuration settings for all access points that join the device, use the **show ap config** command.

```
show ap config {general | global}
```

| Syntax Description | |
|--------------------|---|
| ethernet | Displays ethernet VLAN tagging information for all Cisco APs. |
| general | Displays common information for all Cisco APs. |
| global | Displays global settings for all Cisco APs. |

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

| Command Modes | Any command mode |
|---------------|------------------|
|---------------|------------------|

| Command History | Release | Modification |
|-----------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to display global syslog server settings:

```
Device# show ap config global
```

```
AP global system logging host                : 255.255.255.255
```

show ap config general

To view the general configuration information of all the Cisco APs, use the **show ap config general** command.

show ap config general

| | | |
|---------------------------|--|------------------------------|
| Syntax Description | This command has no keywords or arguments. | |
| Command Default | None | |
| Command Modes | Privileged EXEC (#) | |
| Command History | Release | Modification |
| | Cisco IOS XE Gibraltar 16.11.1 | This command was introduced. |

This example shows how to view the general configuration information of all Cisco APs:

```
Device# show ap config general
Cisco AP Name   : AP4C77.6DF2.D588
=====
<SNIP>
Dhcp Server                : Enabled
```

show ap client-trace events all

To view the AP client trace event information, use the **show ap client-trace events all** command.

show ap client-trace events all

| | |
|---------------------------|--|
| Syntax Description | This command has no keywords or arguments. |
|---------------------------|--|

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

| | |
|----------------------|---------------------|
| Command Modes | Privileged EXEC (#) |
|----------------------|---------------------|

| Command History | Release | Modification |
|------------------------|-------------------------------|------------------------------|
| | Cisco IOS XE Amsterdam 17.2.1 | This command was introduced. |

Examples

This example shows how to view the AP client trace event information:

```
Device# show ap client-trace events all

[*04/29/2019 11:49:21.964964] [AP58AC.78DC.AAA0] [38:e6:0a:ea:99:d4] <aprv0> [D:W]
DOT11_AUTHENTICATION : (.)
[*04/29/2019 11:49:21.972209] [AP58AC.78DC.AAA0] [38:e6:0a:ea:99:d4] <aprv0> [U:W]
DOT11_ASSOC_REQUEST : (.)
[*04/29/2019 11:49:21.972227] [58:ac:78:df:6d:0f] [client] Vendor specific OUI: 00:50:f2
and Type: 02
[*04/29/2019 11:49:21.975975] [AP58AC.78DC.AAA0] [38:e6:0a:ea:99:d4] <aprv0> [D:W]
DOT11_ASSOC_RESPONSE : (.)
```


show ap crash-file

To display the list of both crash and radio core dump files generated by lightweight access points, use the **show ap crash-file** command.

show ap crash-file *chassis chassis-number <1-2>* **active standby**

| Syntax Description | Parameter | Description |
|--------------------|-----------------------|--|
| | chassis | Displays the chassis details. |
| | <i>chassis-number</i> | Specifies the chassis number, either 1 or 2. |
| | active | Specifies an active instance. |
| | standby | Specifies a standby instance. |

Command Default None

Command Modes Any command mode

| Command History | Release | Modification |
|-----------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to display the crash file generated by the access point:

```
Device# show ap crash-file
```

show ap dot11

To view 802.11a or 802.11b or 6-GHz configuration information, use the **show ap dot11** command.

```
show ap dot11 { 24ghz | 5ghz | 6ghz } { channel | coverage | group | load-info | logging |
media-stream | monitor | network | profile | receiver | service-policy | summary | txpower | ccx
global }
```

| Syntax Description | | |
|--------------------|-----------------------|---|
| | 24ghz | Specifies the 2.4-GHz band. |
| | 5ghz | Specifies the 5-GHz band. |
| | 6ghz | Specifies the 6-GHz band. |
| | channel | Displays the automatic channel assignment configuration and statistics. |
| | coverage | Displays the configuration and statistics for coverage hole detection. |
| | group | Displays 802.11a, 6-GHz or 802.11b Cisco radio RF grouping. |
| | load-info | Displays channel utilization and client count information for all Cisco APs. |
| | logging | Displays 802.11a, 6-GHz or 802.11b RF event and performance logging. |
| | media-stream | Display 802.11a, 6-GHz or 802.11b Media Resource Reservation Control configurations. |
| | monitor | Displays the 802.11a, 6-GHz or 802.11b default Cisco radio monitoring. |
| | network | Displays the 802.11a, 6-GHz or 802.11b network configuration. |
| | profile | Displays the 802.11a, 6-GHz or 802.11b lightweight access point performance profiles. |
| | receiver | Displays the configuration and statistics of the 802.11a, 6-GHz or 802.11b receiver. |
| | service-policy | Displays the Quality of Service (QoS) service policies for 802.11a, 6-GHz or 802.11b radio for all Cisco access points. |
| | summary | Displays the 802.11a, 6-GHz or 802.11b Cisco lightweight access point name, channel, and transmit level summary. |
| | txpower | Displays the 802.11a, 6-GHz or 802.11b automatic transmit power assignment. |

ccx global Displays 802.11a, 6-GHz or 802.11b Cisco Client eXtensions (CCX) information for all Cisco access points that are joined to the device.

Command Default

None

Command Modes

Any command mode

Command History

| Release | Modification |
|--|--|
| Cisco IOS XE Gibraltar 16.10.1 Cisco IOS XE Gibraltar 16.12.2s | This command was introduced. |
| | The load-info parameter was added. |
| Cisco IOS XE Cupertino 17.7.1 | This command was modified to include the 6-GHz band. |

This example shows how to display the automatic channel assignment configuration and statistics:

```

Device# show ap dot11 5ghz channel
Automatic Channel Assignment
  Channel Assignment Mode      : AUTO
  Channel Update Interval     : 12 Hours
  Anchor time (Hour of the day) : 20
  Channel Update Contribution  : SNI.
  Channel Assignment Leader    : web (9.9.9.2)
  Last Run                    : 13105 seconds ago
  DCA Sensitivity Level       : MEDIUM (15 dB)
  DCA 802.11n Channel Width   : 40 Mhz
  Channel Energy Levels
    Minimum                   : unknown
    Average                   : unknown
    Maximum                   : unknown
  Channel Dwell Times
    Minimum                   : unknown
    Average                   : unknown
    Maximum                   : unknown
  802.11a 5 GHz Auto-RF Channel List
  Allowed Channel List       : 36,40,44,48,52,56,60,64,149,153,1
57,161
  Unused Channel List       : 100,104,108,112,116,132,136,140,1
65
  802.11a 4.9 GHz Auto-RF Channel List
  Allowed Channel List       :
  Unused Channel List       : 1,2,3,4,5,6,7,8,9,10,11,12,13,14,
15,16,17,18,19,20,21,22,23,24,25,26
  DCA Outdoor AP option     : Disabled
    
```

This example shows how to display the statistics for coverage hole detection:

```

Device# show ap dot11 5ghz coverage
Coverage Hole Detection
  802.11a Coverage Hole Detection Mode : Enabled
  802.11a Coverage Voice Packet Count  : 100 packet(s)
  802.11a Coverage Voice Packet Percentage : 50 %
  802.11a Coverage Voice RSSI Threshold : -80dBm
  802.11a Coverage Data Packet Count   : 50 packet(s)
  802.11a Coverage Data Packet Percentage : 50 %
  802.11a Coverage Data RSSI Threshold : -80dBm
    
```

```
802.11a Global coverage exception level      : 25
802.11a Global client minimum exception level : 3 clients
```

This example shows how to display Cisco radio RF group settings:

```
Device# show ap dot11 5ghz group
```

```
Radio RF Grouping
```

```
802.11a Group Mode           : STATIC
802.11a Group Update Interval : 600 seconds
802.11a Group Leader         : web (10.10.10.1)
802.11a Group Member         : web(10.10.10.1)
                             nb1(172.13.21.45) (*Unreachable)
802.11a Last Run             : 438 seconds ago
```

```
Mobility Agents RF membership information
-----
```

```
No of 802.11a MA RF-members : 0
```

This example shows how to display 802.11a RF event and performance logging:

```
Device# show ap dot11 5ghz logging
```

```
RF Event and Performance Logging
```

```
Channel Update Logging      : Off
Coverage Profile Logging    : Off
Foreign Profile Logging     : Off
Load Profile Logging        : Off
Noise Profile Logging       : Off
Performance Profile Logging : Off
TxPower Update Logging     : Off
```

This example shows how to display the 802.11a media stream configuration:

```
Device# show ap dot11 5ghz media-stream
```

```
Multicast-direct           : Disabled
Best Effort                 : Disabled
Video Re-Direct            : Disabled
Max Allowed Streams Per Radio : Auto
Max Allowed Streams Per Client : Auto
Max Video Bandwidth         : 0
Max Voice Bandwidth         : 75
Max Media Bandwidth         : 85
Min PHY Rate (Kbps)         : 6000
Max Retry Percentage        : 80
```

This example shows how to display the radio monitoring for the 802.11b network:

```
Device# show ap dot11 5ghz monitor
```

```
Default 802.11a AP monitoring
```

```
802.11a Monitor Mode           : Enabled
802.11a Monitor Mode for Mesh AP Backhaul : disabled
802.11a Monitor Channels       : Country channels
802.11a RRM Neighbor Discover Type : Transparent
802.11a AP Coverage Interval   : 180 seconds
802.11a AP Load Interval       : 60 seconds
802.11a AP Noise Interval      : 180 seconds
802.11a AP Signal Strength Interval : 60 seconds
```

This example shows how to display the global configuration and statistics of an 802.11a profile:

```
Device# show ap dot11 5ghz profile
Default 802.11a AP performance profiles
802.11a Global Interference threshold..... 10%
802.11a Global noise threshold..... -70 dBm
802.11a Global RF utilization threshold..... 80%
802.11a Global throughput threshold..... 1000000 bps
802.11a Global clients threshold..... 12 clients
802.11a Global coverage threshold..... 12 dB
802.11a Global coverage exception level..... 80%
802.11a Global client minimum exception lev..... 3 clients
```

This example shows how to display the network configuration of an 802.11a profile:

```
Device# show ap dot11 5ghz network
802.11a Network : Enabled
11nSupport : Enabled
    802.11a Low Band : Enabled
    802.11a Mid Band : Enabled
    802.11a High Band : Enabled

802.11a Operational Rates
    802.11a 6M : Mandatory
    802.11a 9M : Supported
    802.11a 12M : Mandatory
    802.11a 18M : Supported
    802.11a 24M : Mandatory
    802.11a 36M : Supported
    802.11a 48M : Supported
    802.11a 54M : Supported
802.11n MCS Settings:
    MCS 0 : Supported
    MCS 1 : Supported
    MCS 2 : Supported
    MCS 3 : Supported
    MCS 4 : Supported
    MCS 5 : Supported
    MCS 6 : Supported
    MCS 7 : Supported
    MCS 8 : Supported
    MCS 9 : Supported
    MCS 10 : Supported
    MCS 11 : Supported
    MCS 12 : Supported
    MCS 13 : Supported
    MCS 14 : Supported
    MCS 15 : Supported
    MCS 16 : Supported
    MCS 17 : Supported
    MCS 18 : Supported
    MCS 19 : Supported
    MCS 20 : Supported
    MCS 21 : Supported
    MCS 22 : Supported
    MCS 23 : Supported
802.11n Status:
A-MPDU Tx:
    Priority 0 : Enabled
    Priority 1 : Disabled
    Priority 2 : Disabled
    Priority 3 : Disabled
    Priority 4 : Enabled
    Priority 5 : Enabled
```

```

Priority 6 : Disabled
Priority 7 : Disabled
A-MSDU Tx:
Priority 0 : Enabled
Priority 1 : Enabled
Priority 2 : Enabled
Priority 3 : Enabled
Priority 4 : Enabled
Priority 5 : Enabled
Priority 6 : Disabled
Priority 7 : Disabled
Guard Interval : Any
Rifs Rx : Enabled
Beacon Interval : 100
CF Pollable mandatory : Disabled
CF Poll Request Mandatory : Disabled
CFP Period : 4
CFP Maximum Duration : 60
Default Channel : 36
Default Tx Power Level : 1
DTPC Status : Enabled
Fragmentation Threshold : 2346
Pico-Cell Status : Disabled
Pico-Cell-V2 Status : Disabled
TI Threshold : 0
Legacy Tx Beamforming setting : Disabled
Traffic Stream Metrics Status : Disabled
Expedited BW Request Status : Disabled
EDCA profile type check : default-wmm
Call Admission Control (CAC) configuration
Voice AC
Voice AC - Admission control (ACM) : Disabled
Voice Stream-Size : 84000
Voice Max-Streams : 2
Voice Max RF Bandwidth : 75
Voice Reserved Roaming Bandwidth : 6
Voice Load-Based CAC mode : Enabled
Voice tspec inactivity timeout : Enabled
CAC SIP-Voice configuration
SIP based CAC : Disabled
SIP call bandwidth : 64
SIP call bandwidth sample-size : 20
Video AC
Video AC - Admission control (ACM) : Disabled
Video max RF bandwidth : Infinite
Video reserved roaming bandwidth : 0

```

This example shows how to display the global configuration and statistics of an 802.11a profile:

```

Device# show ap dot11 5ghz receiver
Default 802.11a AP performance profiles
802.11a Global Interference threshold..... 10%
802.11a Global noise threshold..... -70 dBm
802.11a Global RF utilization threshold..... 80%
802.11a Global throughput threshold..... 1000000 bps
802.11a Global clients threshold..... 12 clients
802.11a Global coverage threshold..... 12 dB
802.11a Global coverage exception level..... 80%
802.11a Global client minimum exception lev..... 3 clients

```

This example shows how to display the global configuration and statistics of an 802.11a profile:

```
Device# show ap dot11 5ghz service-policy
```

This example shows how to display a summary of the 802.11b access point settings:

```
Device# show ap dot11 5ghz summary
AP Name MAC Address      Admin State Operation State Channel TxPower
-----
CJ-1240 00:21:1b:ea:36:60 ENABLED      UP              161            1 ( )
CJ-1130 00:1f:ca:cf:b6:60 ENABLED      UP              56*            1 (*)
```

This example shows how to display the configuration and statistics of the 802.11a transmit power cost:

```
Device# show ap dot11 5ghz txpower
Automatic Transmit Power Assignment

Transmit Power Assignment Mode      : AUTO
Transmit Power Update Interval     : 600 seconds
Transmit Power Threshold            : -70 dBm
Transmit Power Neighbor Count       : 3 APs
Min Transmit Power                  : -10 dBm
Max Transmit Power                  : 30 dBm
Transmit Power Update Contribution  : SNI.
Transmit Power Assignment Leader    : web (10.10.10.1)
Last Run                            : 437 seconds ago
```

This example shows how to display the configuration and statistics of the 802.11a transmit power cost:

```
Device# show ap dot11 5ghz ccx global
802.11a Client Beacon Measurements:
disabled
```

show ap dot11

To display 802.11 band parameters, use the **show ap dot11** command.

show ap dot11 {24ghz | 5ghz} {media-stream rrc | network | profile | summary}

| | |
|---------------------------|---|
| Syntax Description | <p>media-stream rrc Displays Media Stream configurations.</p> <p>network Shows network configuration.</p> <p>profile Shows profiling information for all Cisco APs.</p> <p>summary Shows configuration and statistics of 802.11b and 802.11a Cisco APs.</p> |
| Command Default | None |
| Command Modes | User EXEC command mode or Privileged EXEC command mode |
| Usage Guidelines | None. |

The following is a sample output of the **show ap dot11 24ghz media-stream rrc** command.

```
Device#show ap dot11 24ghz media-stream rrc

Multicast-direct           : Disabled
Best Effort                 : Disabled
Video Re-Direct            : Disabled
Max Allowed Streams Per Radio : Auto
Max Allowed Streams Per Client : Auto
Max Video Bandwidth         : 0
Max Voice Bandwidth         : 75
Max Media Bandwidth         : 85
Min PHY Rate (Kbps)         : 6000
Max Retry Percentage        : 80
```


show ap dot11 24ghz

To display the 2.4 GHz RRM parameters, use the **show ap dot11 24ghz** command.

```
show ap dot11 24ghz {ccx | channel | coverage | group | l2roam | logging | monitor | profile | receiver
| summary | txpower}
```

| Syntax Description | Option | Description |
|--------------------|-----------------|--|
| | ccx | Displays the 802.11b CCX information for all Cisco APs. |
| | channel | Displays the configuration and statistics of the 802.11b channel assignment. |
| | coverage | Displays the configuration and statistics of the 802.11b coverage. |
| | group | Displays the configuration and statistics of the 802.11b grouping. |
| | l2roam | Displays 802.11b l2roam information. |
| | logging | Displays the configuration and statistics of the 802.11b event logging. |
| | monitor | Displays the configuration and statistics of the 802.11b monitoring. |
| | profile | Displays 802.11b profiling information for all Cisco APs. |
| | receiver | Displays the configuration and statistics of the 802.11b receiver. |
| | summary | Displays the configuration and statistics of the 802.11b Cisco APs. |
| | txpower | Displays the configuration and statistics of the 802.11b transmit power control. |

Command Default None.

Command Modes Global configuration.

| Command History | Release | Modification |
|-----------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

Usage Guidelines None.

This example shows how to display configuration and statistics of the 802.11b coverage.

```
Device#show ap dot11 24ghz coverage
```

```
Coverage Hole Detection
 802.11b Coverage Hole Detection Mode      : Enabled
 802.11b Coverage Voice Packet Count      : 100 packet(s)
 802.11b Coverage Voice Packet Percentage  : 50%
 802.11b Coverage Voice RSSI Threshold    : -80 dBm
 802.11b Coverage Data Packet Count       : 50 packet(s)
 802.11b Coverage Data Packet Percentage  : 50%
 802.11b Coverage Data RSSI Threshold     : -80 dBm
```

```
802.11b Global coverage exception level      : 25 %  
802.11b Global client minimum exception level : 3 clients
```

show ap dot11 24ghz SI config

To see the spectrum intelligence (SI) configuration details for the 2.4-GHz band, use the **show ap dot11 24ghz SI config** command.

```
show ap dot11 24ghz SI config [chassis {chassis-number | active | standby} R0]
```

Syntax Description

chassis-number Chassis number as either 1 or 2.

active R0 Active instance of the configuration in Route-processor slot 0.

standby R0 Standby instance of the configuration in Route-processor slot 0.

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Examples

The following example shows how to see the SI configuration details for the 2.4-GHz band:

```
Device# show ap dot11 24ghz SI config chassis 1 R0
```

show ap dot11 24ghz SI device type

To see the spectrum intelligence (SI) interferers of different types for the 2.4-GHz band, use the **show ap dot11 24ghz SI device type** command.

```
show ap dot11 24ghz SI device type {cont_tx | mw_oven | si_fhss} [chassis {chassis-number
| active | standby} R0]
```

Syntax Description

| | |
|-----------------------|--|
| cont_tx | SI interferers of type Continuous transmitter for the 2.4-GHz band. |
| mw_oven | SI interferers of type microwave oven for the 2.4-GHz band. |
| si_fhss | SI interferers of type Frequency Hopping Spread Spectrum for the 2.4-GHz band. |
| <i>chassis-number</i> | Enter the chassis number as either 1 or 2. |
| active R0 | Active instance of the configuration in Route-processor slot 0. |
| standby R0 | Standby instance of the configuration in Route-processor slot 0. |

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Examples

The following example shows how to see the details of SI interferers of type microwave oven in the 2.4-GHz band:

```
Device# show ap dot11 24ghz SI device type mw_oven chassis 1 R0
```

show ap dot11 5ghz

To display the 5GHz RRM parameters, use the **show ap dot11 5ghz** command.

show ap dot11 5ghz {**ccx** | **channel** | **coverage** | **group** | **l2roam** | **logging** | **monitor** | **profile** | **receiver** | **summary** | **txpower**}

| Syntax Description | Parameter | Description |
|--------------------|-----------------|--|
| | ccx | Displays the 802.11a CCX information for all Cisco APs. |
| | channel | Displays the configuration and statistics of the 802.11a channel assignment. |
| | coverage | Displays the configuration and statistics of the 802.11a coverage. |
| | group | Displays the configuration and statistics of the 802.11a grouping. |
| | l2roam | Displays 802.11a l2roam information. |
| | logging | Displays the configuration and statistics of the 802.11a event logging. |
| | monitor | Displays the configuration and statistics of the 802.11a monitoring. |
| | profile | Displays 802.11a profiling information for all Cisco APs. |
| | receiver | Displays the configuration and statistics of the 802.11a receiver. |
| | summary | Displays the configuration and statistics of the 802.11a Cisco APs. |
| | txpower | Displays the configuration and statistics of the 802.11a transmit power control. |

Command Default None.

Command Modes Global configuration.

| Command History | Release | Modification |
|-----------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

Usage Guidelines None.

This example shows configuration and statistics of 802.11a channel assignment.

```
Device#show ap dot11 5ghz channel
```

```
Automatic Channel Assignment
  Channel Assignment Mode      : AUTO
  Channel Update Interval     : 12 Hours
  Anchor time (Hour of the day) : 20
  Channel Update Contribution  : SNI..
  Channel Assignment Leader    : web (9.9.9.2)
  Last Run                    : 16534 seconds ago
  DCA Sensitivity Level        : MEDIUM (15 dB)
  DCA 802.11n Channel Width   : 40 Mhz
```

```
Channel Energy Levels
  Minimum           : unknown
  Average           : unknown
  Maximum           : unknown
Channel Dwell Times
  Minimum           : unknown
  Average           : unknown
  Maximum           : unknown
802.11a 5 GHz Auto-RF Channel List
Allowed Channel List      : 36,40,44,48,52,56,60,64,149,153,1
                           57,161
Unused Channel List       : 100,104,108,112,116,132,136,140,1
                           65
802.11a 4.9 GHz Auto-RF Channel List
Allowed Channel List      :
Unused Channel List       : 1,2,3,4,5,6,7,8,9,10,11,12,13,14,
                           15,16,17,18,19,20,21,22,23,24,25,26
DCA Outdoor AP option    : Disabled
```

show ap dot11 24ghz cleanair air-quality

To display the air-quality summary information and air-quality worst information for the 802.11 networks, use the **show ap dot11 cleanair** command.

```
show ap dot11 {24ghz | 5ghz | dual-band} cleanair {air-quality | config | device | summary}
```

| Syntax Description | | |
|--------------------|--|--|
| 24ghz | Displays the 2.4 GHz band. | |
| 5ghz | Displays the 5 GHz band. | |
| dual-band | Displays 802.11 dual-band radios. | |
| cleanair | Displays cleanair configurations. | |
| air-quality | Displays the Cleanair Air-Quality (AQ) data for 2.4GHz band. | |
| device | Displays the CleanAir Interferers of device for 2.4GHz band. | |
| config | Displays CleanAir Configuration for 2.4GHz band. | |
| summary | Displays cleanair configurations for all 802.11a Cisco APs. | |

Command Default None

Command Modes Any command mode

| Command History | Release | Modification |
|-----------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to display the worst air-quality information for the 5 GHz band:

```
Device# show ap dot11 5ghz cleanair air-quality worst
```

```
AQ = Air Quality
DFS = Dynamic Frequency Selection
AP Name      Channel Avg AQ Min AQ Interferers DFS
-----
CISCO_AP3500 36      95      70      0          40
```

This example shows how to display the worst air-quality information for the 2.4 GHz band:

```
Device# show ap dot11 24ghz cleanair air-quality worst
```

```
AQ = Air Quality
DFS = Dynamic Frequency Selection
AP Name      Channel Avg AQ Min AQ Interferers DFS
-----
CISCO_AP3500 1        83      57      3          5
```

show ap dot11 24ghz cleanair air-quality

To display the air-quality summary information and air-quality worst information for the 802.11 networks, use the **show ap dot11 cleanair air-quality** command.

show ap dot11 {24ghz | 5ghz} cleanair air-quality {summary | worst}

| Syntax Description | Parameter | Description |
|--------------------|----------------|--|
| | 24ghz | Displays the 2.4 GHz band. |
| | 5ghz | Displays the 5 GHz band. |
| | summary | Displays a summary of 802.11 radio band air-quality information. |
| | worst | Displays the worst air-quality information for 802.11 networks. |

Command Default None

Command Modes Any command mode

| Command History | Release | Modification |
|-----------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to display the worst air-quality information for the 5 GHz band:

```
Device# show ap dot11 5ghz cleanair air-quality worst
```

```
AQ = Air Quality
DFS = Dynamic Frequency Selection
AP Name      Channel Avg AQ Min AQ Interferers DFS
-----
CISCO_AP3500 36      95    70    0          40
```

This example shows how to display the worst air-quality information for the 2.4 GHz band:

```
Device# show ap dot11 24ghz cleanair air-quality worst
```

```
AQ = Air Quality
DFS = Dynamic Frequency Selection
AP Name      Channel Avg AQ Min AQ Interferers DFS
-----
CISCO_AP3500 1        83    57    3          5
```


show ap dot11 cleanair config

To display the CleanAir configuration for the 802.11 networks, use the **show ap dot11 cleanair config** command.

show ap dot11 {24ghz | 5ghz} cleanair config

| Syntax Description | 24ghz Displays the 2.4 GHz band. | | | | |
|--------------------------------|--|---------|--------------|--------------------------------|------------------------------|
| | 5ghz Displays the 5 GHz band. | | | | |
| Command Default | None | | | | |
| Command Modes | Any command mode | | | | |
| Command History | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.10.1</td> <td>This command was introduced.</td> </tr> </tbody> </table> | Release | Modification | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. | | | | |

This example shows how to display the CleanAir configuration for the 2.4 GHz band:

```

Device# show ap dot11 24ghz cleanair config
Clean Air Solution..... : Disabled
Air Quality Settings:
  Air Quality Reporting..... : Disabled
  Air Quality Reporting Period (min)..... : 15
  Air Quality Alarms..... : Enabled
  Air Quality Alarm Threshold..... : 10
Interference Device Settings:
  Interference Device Reporting..... : Enabled
  Bluetooth Link..... : Enabled
  Microwave Oven..... : Enabled
  802.11 FH..... : Enabled
  Bluetooth Discovery..... : Enabled
  TDD Transmitter..... : Enabled
  Jammer..... : Enabled
  Continuous Transmitter..... : Enabled
  DECT-like Phone..... : Enabled
  Video Camera..... : Enabled
  802.15.4..... : Enabled
  WiFi Inverted..... : Enabled
  WiFi Invalid Channel..... : Enabled
  SuperAG..... : Enabled
  Canopy..... : Enabled
  Microsoft Device..... : Enabled
  WiMax Mobile..... : Enabled
  WiMax Fixed..... : Enabled
Interference Device Types Triggering Alarms:
  Bluetooth Link..... : Disabled
  Microwave Oven..... : Disabled
  802.11 FH..... : Disabled
  Bluetooth Discovery..... : Disabled
  TDD Transmitter..... : Disabled
  Jammer..... : Disabled
  Continuous Transmitter..... : Disabled
  DECT-like Phone..... : Disabled
    
```

```
Video Camera..... : Disabled
802.15.4..... : Disabled
WiFi Inverted..... : Enabled
WiFi Invalid Channel..... : Enabled
SuperAG..... : Disabled
Canopy..... : Disabled
Microsoft Device..... : Disabled
WiMax Mobile..... : Disabled
WiMax Fixed..... : Disabled
Interference Device Alarms..... : Enabled
Additional Clean Air Settings:
CleanAir Event-driven RRM State..... : Disabled
CleanAir Driven RRM Sensitivity..... : LOW
CleanAir Persistent Devices state..... : Disabled
```

show ap dot11 cleanair summary

To view CleanAir configurations for all 802.11a Cisco APs, use the **show ap dot11 cleanair summary** command.

```
show ap dot11 {24ghz | 5ghz} cleanair summary
```

| | | |
|---------------------------|-------------------------|--|
| Syntax Description | 24ghz | Specifies the 2.4-GHz band |
| | 5ghz | Specifies the 5-GHz band |
| | cleanair summary | Summary of CleanAir configurations for all 802.11a Cisco APs |
| Command Default | None | |
| Command Modes | Any command mode | |
| Command History | Release | Modification |
| | | This command was introduced. |

show ap dot11 dual-band summary

To view a brief summary of access points with dual-band radios, use the **show ap dot11 dual-band summary** command.

show ap dot11 dual-band summary

| | |
|---------------------------|--|
| Syntax Description | This command has no keywords or arguments. |
|---------------------------|--|

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

| | |
|----------------------|-----------------|
| Command Modes | Privileged EXEC |
|----------------------|-----------------|

| Command History | Release | Modification |
|------------------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.12.1 | This command was introduced. |

Example

The following example shows how to view brief summary of tag names:

```
Device# show ap dot11 dual-band summary
```

show ap environment

To see the AP environment information of all APs, use the **show ap environment** command.

show ap environment [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

Syntax Description

chassis-number Enter the chassis number as either 1 or 2.

active R0 Active instance of the AP filters in Route-processor slot 0.

standby R0 Standby instance of the AP filters in Route-processor slot 0.

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Examples

The following example shows how to see the AP environment information:

```
Device# show ap environment
```

show ap file-transfer https summary

To view the summary of AP file transfer using HTTPS, use the **show ap file-transfer https summary** command in privileged EXEC mode.

show ap file-transfer https summary

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC (#)

| Command History | Release | Modification |
|-----------------|-----------------------------|------------------------------|
| | Cisco IOS XE Dublin 17.11.1 | This command was introduced. |

Examples

The following example shows how to view the summary of AP file transfer using HTTPS:

```
Device# show ap file-transfer https summary
```

```
Configured port      : 8443
Operational port     : 8443
```

show ap filters active

To see the details of active AP filters, use the **show ap filters active** command.

```
show ap filters active [chassis {chassis-number | active | standby} R0]
```

Syntax Description

chassis-number Chassis number as either 1 or 2.

active R0 Active instance of the active AP filters in Route-processor slot 0.

standby R0 Standby instance of the active AP filters in Route-processor slot 0.

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Examples

The following example shows how to see the details of the active AP filters for the active instance:

```
Device# show ap filters active chassis active R0
```

show ap filters active type priming

To display the list of all the active priming filters, use the **show ap filters active type priming** command.

show ap filters active type priming

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Privileged EXEC (#)

Command History

| Release | Modification |
|-------------------------------|------------------------------|
| Cisco IOS XE Cupertino 17.9.2 | This command was introduced. |

Examples

The following example shows how to display the list of all the active priming filters:

```
Device# show ap filters active type priming
```

| Priority | Filter Name | regex | Priming profile |
|----------|-------------|--------------|-----------------|
| 0 | FLR2 | *AP-FLOOR-2* | AP-PRIMING-2 |
| 1 | FLR1 | *AP-FLOOR-1* | AP-PRIMING-1 |

show ap filters all

To see the details of all AP filters, use the **show ap filters all** command.

show ap filters all [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

Syntax Description

chassis-number Enter the chassis number as either 1 or 2.

active R0 Active instance of the AP filters in Route-processor slot 0.

standby R0 Standby instance of the AP filters in Route-processor slot 0.

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Examples

The following example shows how to see the details of all the AP filters for the active instance:

```
Device# show ap filters all chassis active R0
```

show ap filters all type priming

To display the list of all the priming filters, use the **show ap filters all type priming** command.

show ap filters all type priming

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Privileged EXEC (#)

| Command History | Release | Modification |
|-----------------|-------------------------------|------------------------------|
| | Cisco IOS XE Cupertino 17.9.2 | This command was introduced. |

Examples

The following example shows how to display the list of all the priming filters:

```
Device# show ap filters all type priming
```

| Filter Name | regex | Priming profile |
|-------------|--------------|-----------------|
| FLR1 | *AP-FLOOR-1* | AP-PRIMING-1 |
| FLR2 | *AP-FLOOR-2* | AP-PRIMING-2 |

show ap fra

To see the flexible radio assignment (FRA) configurations in APs, use the **show ap fra** command.

```
show ap fra [chassis {chassis-number | active | standby} R0]
```

Syntax Description

chassis-number Chassis number as either 1 or 2.

active R0 Active instance in Route-processor slot 0.

standby R0 Standby instance in Route-processor slot 0.

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Examples

The following example shows how to see the FRA configurations in APs:

```
Device# show ap fra
```

show ap fra 5-6ghz

To view the Flexible Radio Assignment (FRA) 5/6-GHz configurations, use the **show ap fra 5-6ghz** command.

show ap fra 5-6ghz

| | | |
|---------------------------|--|------------------------------|
| Syntax Description | This command has no keywords or arguments. | |
| Command Default | None | |
| Command Modes | Privileged EXEC # | |
| Command History | Release | Modification |
| | Cisco IOS XE Cupertino 17.9.1 | This command was introduced. |

Example

This example shows how to view the Flexible Radio Assignment (FRA) 5/6-GHz configurations:

```
Device# show ap fra 5-6ghz
```

show ap geolocation ranging

To view the AP geolocation ranging information, use the **show ap geolocation ranging** { command.

| | |
|---------------------------|--|
| Syntax Description | report Displays the AP geolocation ranging reports. |
| | request Displays the AP geolocation ranging requests. |

Command Default None

Command Modes Privileged EXEC (#)

| Command History | Release | Modification |
|------------------------|-----------------------------|------------------------------|
| | Cisco IOS XE Dublin 17.12.1 | This command was introduced. |

Example

This example shows how to view the AP geolocation ranging information:

```
Device# show ap geolocation ranging report
Device# show ap geolocation ranging request
```

show ap gps location

To see the GPS location of all APs, use the **show ap gps location** command.

show ap gps location [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

Syntax Description

chassis-number Enter the chassis number as either 1 or 2.

active R0 Active instance of the AP filters in Route-processor slot 0.

standby R0 Standby instance of the AP filters in Route-processor slot 0.

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Examples

The following example shows how to see the GPS location of all APs:

```
Device# show ap gps location
```

show ap grpc summary

To display the status summary of GRPC channel from the AP to Cisco DNA, use the **show ap grpc summary** command.

show ap grpc summary

| | | |
|---------------------------|--------------------------------|------------------------------|
| Syntax Description | This command has no arguments. | |
| Command Default | None | |
| Command Modes | Privileged EXEC (#) | |
| Command History | Release | Modification |
| | Cisco IOS XE Amsterdam 17.3.1 | This command was introduced. |
| Usage Guidelines | None | |

Example

The following example shows how to display the status summary of GRPC channel from the AP to Cisco DNA:

```
Device(config)# show ap grpc summary
```

show ap group hyperlocation

To view a summary or detailed information of Hyperlocation configuration for an AP group, use the **show ap group *ap-group-name* hyperlocation** command.

show ap group hyperlocation {summary | detail}

| Syntax Description | summary | Shows the overall configuration values (AP group specific) and operational status and parameters for the AP group. |
|--------------------|------------------------------|--|
| | detail | Shows both overall (AP group specific) and per-AP configuration values and operational status for the AP group. The APs listed are only those that belong to the AP group. |
| Command Modes | User EXEC Privileged EXEC | |
| Command History | Release | Modification |
| | Cisco IOS XE Denali 16.3.1 | This command was introduced. |

This example shows how to view a summary of Hyperlocation configuration for an AP group:

```
Device# show ap group my-ap-group hyperlocation summary

Site Name: my-ap-group
Site Description: This is an AP group
Hyperlocation operational status: Up
Reason: N/A
Hyperlocation NTP server: 9.0.0.4
Hyperlocation admin status: Enabled
Hyperlocation detection threshold: -100 dBm
Hyperlocation trigger threshold: 11
Hyperlocation reset threshold: 9
```



Note For Hyperlocation to be operational, the following conditions must be met:

- At least one Cisco CMX with Hyperlocation enabled
- Hyperlocation admin state operational
- Either AP NTP or IOS NTP configured

This example shows how to view detailed information about Hyperlocation configuration for an AP group:


```
Device# show ap group my-ap-group hyperlocation detail
```

```
Site Name: my-ap-group
Site Description: This is an AP group
Hyperlocation operational status: Up
Reason: N/A
Hyperlocation NTP server: 9.0.0.4
Hyperlocation admin status: Enabled
Hyperlocation detection threshold: -100 dBm
Hyperlocation trigger threshold: 11
Hyperlocation reset threshold: 9
```

```
Values for APs in all AP Groups:
```

| AP Name | Radio MAC | Method | Hyperlocation |
|------------------|----------------|--------|---------------|
| APf07f.0635.2d40 | f07f.0676.3b89 | WSM | Enabled |
| APf4cf.e272.4ed0 | f4cf.e223.ba31 | Local | Enabled |

show history channel interface dot11Radio all

To check channel change or trigger reason and history, use the **show history channel interface dot11Radio all** command.

show history channel interface dot11Radio all

| | | |
|---------------------------|--|------------------------------|
| Syntax Description | This command has no keywords or arguments. | |
| Command Default | None | |
| Command Modes | Privileged EXEC (#) | |
| Command History | Release | Modification |
| | Cisco IOS XE Amsterdam 17.2.1 | This command was introduced. |

Examples

This example shows how to check channel change or trigger reason and history:

```
Device# show history channel interface dot11Radio all

          Timestamp Slot Client count Channel Trigger
Fri May 31 12:57:04 2019    0         0      11 RRM-DCA
Fri May 31 13:10:02 2019    0         0       1 RRM-DCA
Fri May 31 12:57:04 2019    1         0       60 Manual
Fri May 31 13:00:16 2019    1         0      149   DFS
```

show ap hyperlocation

To view a summary or detailed information about the hyperlocation configuration, use the **show ap hyperlocation** command.

show ap hyperlocation {**summary** | **detail**}

| Syntax Description | | |
|--------------------|----------------|---|
| | summary | Shows the overall configuration and operational values. |
| | detail | Shows the overall configuration and operation values as well as detailed information about each AP. |

Command Default None

| Command History | Release | Modification |
|-----------------|----------------------------|---|
| | Cisco IOS XE Denali 16.2.1 | This command was introduced. |
| | Cisco IOS XE Denali 16.3.1 | This command was modified. The ble-beacon keyword was added. |

Usage Guidelines For hyperlocation to be operational, the following conditions must be met:

- At least one Cisco Connected Mobile Experiences (CMX) must be present with hyperlocation enabled.
- The hyperlocation admin state should be operational.
- Either AP Network Time Protocol (NTP) or IOS NTP should be configured.

Example

This example shows how to view a summary of the hyperlocation configuration:

```
Device# show ap hyperlocation summary

Hyperlocation operational status: Up
Hyperlocation NTP server currently used: 9.0.0.4
Hyperlocation admin status: Enabled
Hyperlocation detection threshold: -100 dBm
Hyperlocation trigger threshold: 10
Hyperlocation reset threshold: 8
```

This example shows how to view detailed information about hyperlocation configuration:

```
Device# show ap hyperlocation detail

Hyperlocation operational status: Up
Hyperlocation NTP server currently used: 9.0.0.4
Hyperlocation admin status: Enabled
Hyperlocation detection threshold: -100 dBm
Hyperlocation trigger threshold: 10
Hyperlocation reset threshold: 8
```

show ap hyperlocation

| AP Name | Radio MAC | Method | Hyperlocation |
|------------------|----------------|--------|---------------|
| AP84b8.0252.b930 | 84b8.0216.c721 | HALO | Enabled |
| AP84b8.0265.5540 | 84b8.0243.8796 | WSM | Enabled |
| APf07f.0635.2d40 | f07f.0676.3b89 | WSM | Enabled |
| APf4cf.e272.4ed0 | f4cf.e223.ba31 | HALO | Enabled |

show ap hyperlocation cmx summary

To see a summary of CMX information with Hyperlocation enabled, use the **show ap hyperlocation cmx summary** command.

```
show ap hyperlocation cmx summary [chassis {chassis-number | active | standby} R0]
```

Syntax Description

chassis-number Enter the chassis number as either 1 or 2.

active R0 Active instance of the AP filters in Route-processor slot 0.

standby R0 Standby instance of the AP filters in Route-processor slot 0.

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Examples

The following example shows how to see a summary of CMX information with Hyperlocation enabled:

```
Device# show ap hyperlocation cmx summary
```

show ap image

To display the images present on Cisco lightweight access points, use the **show ap image** command.

show ap image

| | | |
|---------------------------|---|------------------------------|
| Syntax Description | This command has no keywords and arguments. | |
| Command Default | None | |
| Command Modes | Any command mode | |
| Command History | Release | Modification |
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to display images on the access points:

```
Device# show ap image
```

show ap image file summary

To see the summary of an access point's (AP) software install files, use the **show ap image file summary** command.

show ap image file summary

| | |
|---------------------------|--|
| Syntax Description | This command has no keywords or arguments. |
|---------------------------|--|

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

| | |
|----------------------|---------------------|
| Command Modes | Privileged EXEC (#) |
|----------------------|---------------------|

| Command History | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Bengaluru 17.4.1</td> <td>This command was modified.</td> </tr> </tbody> </table> | Release | Modification | Cisco IOS XE Bengaluru 17.4.1 | This command was modified. |
|-------------------------------|---|---------|--------------|-------------------------------|----------------------------|
| Release | Modification | | | | |
| Cisco IOS XE Bengaluru 17.4.1 | This command was modified. | | | | |

Example

The following example shows how to display the summary of an AP's software install files:

```
Device# show ap image file summary
AP Image Active List
=====
Install File Name: base_image.bin
-----
AP Image Type      Capwap Version Size (KB) Supported AP models
-----
      ap1g1         17.3.0.30      13300  NA
      ap1g2         17.3.0.30  34324      NA
      ap1g3         17.3.0.30  98549      AP803
      ap1g4         17.3.0.30      34324      AP1852E, AP1852I, AP1832I, AP1830I, AP1810W,
OEAP1810
      ap1g5         17.3.0.30      23492      AP1815W, AP1815T, OEAP1815, AP1815I, AP1800I,
AP1800S, AP1815M, 1542D, AP1542I, AP1100AC, AP1101AC, AP1840I
      ap1g6         17.3.0.30  93472      AP2900I, C9117AXI
      ap1g6a        17.3.0.30  247377      C9130AXI, C9130AXE, C9140AXI, C9140AXD,
C9140AXT
      ap1g7         17.3.0.30  23988      AP1900I, C9115AXI, AP1900E, C9115AXE, C9120AXE,
C9120AXP, C9120AXI
      ap1g8         17.3.0.30  23473      C9105AXI, C9105AXW, C9110AXI, C9110AXE
      ap3g1         17.3.0.30  23422      NA
      ap3g2         17.3.0.30  23411  AP1702I
```

show ap image file summary

```

ap3g3      17.3.0.30   23090  AP3802E, AP3802I, AP3802P, AP4800, AP2802E, AP2802I,
AP2802H, AP3800, AP1562E, AP1562I, AP1562D, AP1562PS, IW-6300H-DC, IW-6300H-AC, IW-6300H-DCW,
ESW-6300

c1570      17.3.0.30   13000  AP1572E, 1573E, AP1572I

c3700      17.3.0.30   14032  AP3702E, AP3701E, AP3701I, AP3702I, AP3701P, AP3702P,
AP2702E, AP2702I, AP3702, IW3702, AP3701, AP3700C

virtApImg  17.3.0.30           177056  APVIRTUAL

```

AP Image Prepare List**

```

=====
Install File Name: base_image.bin
-----
=====

```

```

Install File Name: base_image.bin
-----

```

| AP Image Type | Capwap Version | Size (KB) | Supported AP models |
|---------------|----------------|-----------|---|
| ap1g1 | 17.3.0.30 | 13300 | NA |
| ap1g2 | 17.3.0.30 | 34324 | NA |
| ap1g3 | 17.3.0.30 | 98549 | AP803 |
| ap1g4 | 17.3.0.30 | 34324 | AP1852E, AP1852I, AP1832I, AP1830I, AP1810W, OEAP1810 |
| ap1g5 | 17.3.0.30 | 23492 | AP1815W, AP1815T, OEAP1815, AP1815I, AP1800I, AP1800S, AP1815M, 1542D, AP1542I, AP1100AC, AP1101AC, AP1840I |
| ap1g6 | 17.3.0.30 | 93472 | AP2900I, C9117AXI |
| ap1g6a | 17.3.0.30 | 247377 | C9130AXI, C9130AXE, C9140AXI, C9140AXD, C9140AXT |
| ap1g7 | 17.3.0.30 | 23988 | AP1900I, C9115AXI, AP1900E, C9115AXE, C9120AXE, C9120AXP, C9120AXI |
| ap1g8 | 17.3.0.30 | 23473 | C9105AXI, C9105AXW, C9110AXI, C9110AXE |
| ap3g1 | 17.3.0.30 | 23422 | NA |
| ap3g2 | 17.3.0.30 | 23411 | AP1702I |
| ap3g3 | 17.3.0.30 | 23090 | AP3802E, AP3802I, AP3802P, AP4800, AP2802E, AP2802I, AP2802H, AP3800, AP1562E, AP1562I, AP1562D, AP1562PS, IW-6300H-DC, IW-6300H-AC, IW-6300H-DCW, ESW-6300 |
| c1570 | 17.3.0.30 | 13000 | AP1572E, 1573E, AP1572I |
| c3700 | 17.3.0.30 | 14032 | AP3702E, AP3701E, AP3701I, AP3702I, AP3701P, AP3702P, AP2702E, AP2702I, AP3702, IW3702, AP3701, AP3700C |
| virtApImg | 17.3.0.30 | 177056 | APVIRTUAL |

**Difference of Active and Prepare list gives images being predownloaded to Access Points.

show ap image site summary

To see the summary of an access point's (AP) site-filtered upgrades, use the **show ap image site summary** command.

show ap image site summary

| | |
|---------------------------|--|
| Syntax Description | This command has no keywords or arguments. |
|---------------------------|--|

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

| | |
|----------------------|---------------------|
| Command Modes | Privileged EXEC (#) |
|----------------------|---------------------|

| | | |
|------------------------|--------------------------------|------------------------------|
| Command History | Release | Modification |
| | Cisco IOS XE Gibraltar 16.11.1 | This command was introduced. |

Example

The following example shows how to display the summary of an AP's site-filtered upgrades:

```
Device# show ap image site summary
```

```
Image name: smul.bin
Site Tag      Prepared      Activated      Committed
-----
BGL18         yes          ongoing        no
BGL17         yes          ongoing        no
```

show ap iot-radio firmware summary

To display the IoT radio firmware information summary of the access point, use the **show ap iot-radio firmware summary** command.

show ap iot-radio firmware summary

| | |
|---------------------------|--------------------------------|
| Syntax Description | This command has no arguments. |
|---------------------------|--------------------------------|

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

| | |
|----------------------|---------------------|
| Command Modes | Privileged EXEC (#) |
|----------------------|---------------------|

| Command History | Release | Modification |
|------------------------|-------------------------------|------------------------------|
| | Cisco IOS XE Cupertino 17.7.1 | This command was introduced. |

Example

This example shows you how to display the IoT radio firmware information summary of the access point:

```
Device# show ap iot-radio firmware summary
```

show ap link-encryption

To display the link encryption status, use the **show ap link-encryption** command.

show ap link-encryption[{**chassis** | {*chassis-number* | **active** | **standby**} | **R0**}]

Syntax Description

chassis-number Chassis number as either 1 or 2.

active R0 Active instance in Route-processor slot 0.

standby R0 Standby instance in Route-processor slot 0.

Command Default

None

Command Modes

Any command mode

Command History

Release

Modification

Cisco IOS XE Gibraltar 16.10.1 This command was introduced.

This example show how to display the link-encryption status:

```
Device# show Cisco IOS XE Gibraltar 16.12.2s link-encryption
```

show ap lldp neighbors detail

To view the details of the AP Link Layer Discovery Protocol (LLDP) neighbor information on the controller, when the AP is connected to the third-party switch.

show ap lldp neighbors detail

| | | |
|---------------------------|--------------------------------|------------------------------|
| Syntax Description | This command has no arguments. | |
| Command Default | None | |
| Command Default | None | |
| Command Modes | Privileged EXEC | |
| Command History | Release | Modification |
| | Cisco IOS XE Bengaluru 17.5.1 | This command was introduced. |
| Usage Guidelines | None | |

Example

The following example shows how to view the details of AP Link Layer Discovery Protocol (LLDP) neighbor information on the controller, when the AP is connected to the third-party switch:

```
Device# show ap lldp neighbors detail
Number of neighbors: 1
AP Name           : 9130-ap1
AP Interface      : GigabitEthernet0
-----
Neighbor MAC      : c89c.1db1.1f80
Neighbor Name     : flex-ctrl-switch
System Description : Cisco IOS Software, C3750E Software (C3750E-UNIVERSALK9-M), Version
                  15.2(4)E6, RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Thu 05-Apr-18 02:22 by prod_rel_team
Port ID           : Gi1/0/15
Port Description  : 9130-ap2
Chassis Alias    :
Management Addresses :
  IPv4 address    : None
  IPv6 address    : None
Capabilities     :
  Bridge
  Router
Last updated time : 12/02/2020 09:15:48
```

show ap lldp neighbors

To view the AP Link Layer Discovery Protocol (LLDP) neighbor information on the controller, when the AP is connected to the third-party switch.

show ap lldp neighbors

| | | |
|---------------------------|--------------------------------|------------------------------|
| Syntax Description | This command has no arguments. | |
| Command Default | None | |
| Command Modes | Privileged EXEC | |
| Command History | Release | Modification |
| | Cisco IOS XE Bengaluru 17.5.1 | This command was introduced. |
| Usage Guidelines | None | |

Example

The following example shows how to view the AP Link Layer Discovery Protocol (LLDP) neighbor information on the controller, when the AP is connected to the third-party switch:

```
Device# show ap lldp neighbors
```

```
Capability Codes:
```

```
(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
```

| AP Name | AP Interface | Neighbor Name | Neighbor MAC | Port ID | Mgmt. Address | Capabilities | Last updated time |
|----------|------------------|---------------|----------------|----------|---------------|--------------|---------------------|
| 9130-ap1 | GigabitEthernet0 | switch | cxxx.1dxx.1fxx | Gi1/0/15 | None | B R | 12/02/2020 09:15:48 |
| 9117-ap1 | GigabitEthernet0 | switch | cxxx.1dxx.1fxx | Gi1/0/19 | None | B R | 12/02/2020 09:15:47 |

show ap name dot11 neighbor summary

To view the neighbor summary of an access point (AP) in a 802.11 2.4-GHz, 5-GHz, or a 6-GHz network, use the **show ap name *ap-name* dot11 {24ghz | 5ghz | 6ghz} neighbor summary** command.

show ap name dot11 {24ghz | 5ghz | 6ghz} neighbor summary

| | |
|---------------------------|--|
| Syntax Description | <i>ap-name</i> Specifies the Name of the AP. |
|---------------------------|--|

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

| | |
|----------------------|---------------------|
| Command Modes | Privileged EXEC (#) |
|----------------------|---------------------|

| | | |
|------------------------|-------------------------------|------------------------------|
| Command History | Release | Modification |
| | Cisco IOS XE Cupertino 17.7.1 | This command was introduced. |

Examples

This example shows how to view the neighbor summary of the 802.11 2.4-GHz parameter:

```
Device# show ap name AP687D.B45C.0554 dot11 24ghz neighbor summary
```

| BSSID | Channel | Channel-width | Slot | RSSI | Last-Heard | SSID | Neighbor |
|----------------|---------|---------------|------|------|---------------------|------------|----------|
| 10f9.2077.6140 | 1 | 20 Mhz | 0 | -28 | 06/23/2021 01:42:51 | mdns-psk | TRUE |
| 10f9.2077.614f | 1 | 20 Mhz | 0 | -28 | 06/23/2021 01:42:51 | mdns-psk | TRUE |
| 00b0.e192.9600 | 11 | 20 Mhz | 0 | -31 | 06/23/2021 01:42:51 | mdns-psk | TRUE |
| 00b0.e192.960f | 11 | 20 Mhz | 0 | -31 | 06/23/2021 01:42:51 | mdns-psk | TRUE |
| 00ee.ab18.bf0f | 6 | 20 Mhz | 0 | -38 | 06/23/2021 01:42:51 | mdns-psk | TRUE |
| f4db.e69f.8860 | 1 | 20 Mhz | 0 | -75 | 06/23/2021 01:43:06 | wlan1 | FALSE |
| 68ca.e43f.b902 | 1 | 20 Mhz | 0 | -77 | 06/23/2021 01:43:06 | amaz-open | FALSE |
| 68ca.e43f.b900 | 1 | 20 Mhz | 0 | -78 | 06/23/2021 01:43:06 | amaz-web | FALSE |
| 68ca.e43f.b903 | 1 | 20 Mhz | 0 | -78 | 06/23/2021 01:43:06 | amaz-8021x | FALSE |

This example shows how to view the neighbor summary of the 802.11 5-GHz parameter:

```
Device# show ap name AP1117Q.B22U.0221 dot11 5ghz neighbor summary
```

| BSSID | Channel | Channel-width | Slot | RSSI | Last-Heard | SSID | Neighbor |
|----------------|---------|---------------|------|------|--------------------|----------|----------|
| 7872.5dee.496f | 100 | 80 Mhz | 1 | 34 | 6/23/2021 01:43:35 | mdns-psk | FALSE |

This example shows how to view the neighbor summary of the 802.11 6-GHz parameter:

```
Device# show ap name AP1117Q.B22U.0221 dot11 6ghz neighbor summary
```

| BSSID | Channel | Channel-width | Slot | RSSI | Last-Heard | SSID | Neighbor |
|-------|---------|---------------|------|------|------------|------|----------|
|-------|---------|---------------|------|------|------------|------|----------|

| | | | | | | | |
|----------------|---|--------|---|-----|---------------------|-----------|------|
| 687d.b45e.4c53 | 1 | 20 Mhz | 3 | -37 | 06/23/2021 01:42:51 | wpa3-6ghz | TRUE |
| 687d.b45e.53d3 | 1 | 20 Mhz | 3 | -39 | 06/23/2021 01:42:51 | wpa3-6ghz | TRUE |

show ap name lldp neighbors detail

To view the details of the AP Link Layer Discovery Protocol (LLDP) neighbor information on the controller, for a specific AP, when the AP is connected to the third-party switch.

show ap name *ap-name* **lldp neighbors detail**

| | |
|---------------------------|--------------------------------|
| Syntax Description | This command has no arguments. |
|---------------------------|--------------------------------|

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

| | |
|----------------------|-----------------|
| Command Modes | Privileged EXEC |
|----------------------|-----------------|

| Command History | Release | Modification |
|------------------------|-------------------------------|------------------------------|
| | Cisco IOS XE Bengaluru 17.5.1 | This command was introduced. |

| | |
|-------------------------|------|
| Usage Guidelines | None |
|-------------------------|------|

Example

The following example shows how to view the details of the AP Link Layer Discovery Protocol (LLDP) neighbor information on the controller, for a specific AP, when the AP is connected to the third-party switch:

```
Device# show ap name 9130-ap1 lldp neighbors detail
AP Name           : 9130-ap1
AP Interface      : GigabitEthernet0
-----
Neighbor MAC      : c89c.1db1.1f80
Neighbor Name     : flex-ctrl-switch
System Description : Cisco IOS Software, C3750E Software (C3750E-UNIVERSALK9-M), Version
                  15.2(4)E6, RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Thu 05-Apr-18 02:22 by prod_rel_team
Port ID           : Gi1/0/15
Port Description  : 9130-ap2
Chassis Alias     :
Management Addresses :
  IPv4 address    : None
  IPv6 address    : None
Capabilities      :
  Bridge
  Router
Last updated time : 12/02/2020 09:15:48
```


show ap name lldp neighbors

To view the AP Link Layer Discovery Protocol (LLDP) neighbor information on the controller, for a specific AP, when the AP is connected to the third-party switch.

show ap name *ap-name* **lldp neighbors**

| | | |
|---------------------------|--------------------------------|------------------------------|
| Syntax Description | This command has no arguments. | |
| Command Default | None | |
| Command Modes | Privileged EXEC | |
| Command History | Release | Modification |
| | Cisco IOS XE Bengaluru 17.5.1 | This command was introduced. |
| Usage Guidelines | None | |

Example

The following example shows how to view the AP Link Layer Discovery Protocol (LLDP) neighbor information on the controller, for a specific AP, when the AP is connected to the third-party switch:

```
Device# show ap name 9130-ap1 lldp neighbors
AP Name           : 9130-ap1
AP Interface      : GigabitEthernet0
-----
Neighbor MAC      : c89c.1db1.1f80
Neighbor Name     : flex-ctrl-switch
System Description : Cisco IOS Software, C3750E Software (C3750E-UNIVERSALK9-M), Version
                  15.2(4)E6, RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Thu 05-Apr-18 02:22 02:22 by prod_rel_team
Port ID           : Gi1/0/15
Port Description  : 9130-ap2
Chassis Alias     :
Management Addresses :
  IPv4 address    : None
  IPv6 address    : None
Capabilities      :
  Bridge
  Router
Last updated time : 12/02/2020 09:15:48
```

show ap name mesh roam history

To display the roaming history of a mesh AP, use the **show ap name** *cisco-ap-name* **mesh roam history** command.

show ap name *cisco-ap-name* **mesh roam history**

| | |
|---------------------------|---|
| Syntax Description | <i>cisco-ap-name</i> Specifies the Cisco AP name. |
|---------------------------|---|

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

| | |
|----------------------|---------------------|
| Command Modes | Privileged EXEC (#) |
|----------------------|---------------------|

| Command History | Release | Modification |
|------------------------|-----------------------------|------------------------------|
| | Cisco IOS XE Dublin 17.12.1 | This command was introduced. |

Example

The following example shows how to view the roaming history of a mesh AP:

```
Device# show ap name cisco-ap-name mesh roam history
```

show ap name ntp status

To display the Network Time Protocol (NTP) status of an AP, use the **show ap name ntp status** command.

show ap name *ap-name* **ntp status**

| | |
|---------------------------|-------------------------|
| Syntax Description | <i>ap-name</i> AP name. |
|---------------------------|-------------------------|

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

| | |
|----------------------|---------------------|
| Command Modes | Privileged EXEC (#) |
|----------------------|---------------------|

| Command History | Release | Modification |
|------------------------|-------------------------------|------------------------------|
| | Cisco IOS XE Bengaluru 17.6.1 | This command was introduced. |

Examples

The following example shows how to view the NTP status of an AP:

```
Device# show ap name AP-G1-230 ntp status
```

| ap-name | enabled | v4/v6 | IPAddress | Status | Stratum | LastSync | SyncOffset |
|-----------|---------|-------|--------------|----------|---------|----------|------------|
| AP-G1-230 | Y | v4 | 198.51.100.5 | AuthFail | 4 | 1000 | 100 |

show ap ntp status

To display the Network Time Protocol (NTP) status for all the APs, use the **show ap name ntp status** command.

show ap ntp status

Syntax Description This command has no keywords and arguments.

Command Default None

Command Modes Privileged EXEC (#)

| Command History | Release | Modification |
|-----------------|-------------------------------|------------------------------|
| | Cisco IOS XE Bengaluru 17.6.1 | This command was introduced. |

Examples

The following example shows how to view the NTP status for all the APs:

```
Device# show ap ntp status
```

| ap-name | enabled | v4/v6 | IPAddress | Status | Stratum | LastSync | SyncOffset |
|-----------|---------|-------|---------------|----------|---------|----------|------------|
| AP-G1-230 | Y | v4 | 198.51.100.5 | AuthFail | 2 | Never | |
| AP-G1-231 | Y | v4 | 198.51.100.10 | Synced | 3 | 1000 | 100 |
| AP-G1-232 | Y | v4 | 198.51.100.15 | Synced | 16 | 2000 | 50 |

show ap primary list

To see the AP primary list, use the **show ap primary list** command.

```
show ap primary list [{ chassis | { chassis-number | active | standby } | R0 }]
```

Syntax Description

chassis-number Chassis number as either 1 or 2.

active R0 Active instance in Route-processor slot 0.

standby R0 Standby instance in Route-processor slot 0.

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Examples

The following example shows how to see the AP primary list:

```
Device# show ap primary list
```

show ap mesh cac access

To view the number of active calls on access radio for a given AP and its Mesh tree, use **show ap mesh cac access** command.

show ap *ap-name* **mesh cac access**

| Syntax Description | |
|--------------------|---------------------------|
| <i>ap-name</i> | Name of the access point. |

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

| Command Modes | |
|---------------|---------------------|
| | Privileged EXEC (#) |

| Command History | Release | Modification |
|-----------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.11.1 | This command was introduced. |

Usage Guidelines

Example

This example shows how to display the number of active calls on access radio for a given AP and its Mesh tree:

```
Device# show ap <ap-name> mesh cac access
```

| Depth | AP Name | Slot | Radio | BW Used | Call |
|-------|-------------------|------|-----------|---------|------|
| 0 | AALUKKAL-1562-RAP | 0 | 802.11b/g | 0 | 0 |
| | | 1 | 802.11a | 0 | 0 |
| 1 | AP380E.4DBF.C6B0 | 0 | 802.11b/g | 1072 | 2 |
| | | 1 | 802.11a | 0 | 0 |

show ap mesh cac bwused voice

To view the voice bandwidth utilization of a given AP and its Mesh tree, use the **show ap mesh cac bwused voice** command.

show ap *ap-name* **mesh cac bwused voice**

Syntax Description

ap-name Name of the access point.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Example

This example shows how to display the voice bandwidth utilization of a given AP and its Mesh tree:

Device# **show ap <ap-name> mesh cac bwused voice**

| Depth | AP Name | Slot | Radio | BW Used |
|-------|------------------|------|-----------|---------|
| 1 | APA023.9FA9.D920 | 0 | 802.11b/g | 1140 |
| | | 1 | 802.11a | 0 |
| 2 | AP380E.4DBF.C80C | 0 | 802.11b/g | 570 |
| | | 1 | 802.11a | 2144 |
| 2 | AP380E.4DBF.C816 | 0 | 802.11b/g | 0 |
| | | 1 | 802.11a | 0 |
| 2 | APA023.9FA9.B702 | 0 | 802.11b/g | 0 |
| | | 1 | 802.11a | 0 |

show ap mesh cac callpath

To view the number of active calls in access as well as backhaul for a given AP and its Mesh tree, use the **show ap mesh cac callpath** command.

show ap *ap-name* **mesh cac callpath**

| | |
|---------------------------|--|
| Syntax Description | <i>ap-name</i> Name of the access point. |
|---------------------------|--|

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

| | |
|----------------------|---------------------|
| Command Modes | Privileged EXEC (#) |
|----------------------|---------------------|

| Command History | Release | Modification |
|------------------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.11.1 | This command was introduced. |

Usage Guidelines

Example

This example shows how to display the number of active calls in access as well as backhaul for a given AP and its Mesh tree:

```
Device# show ap <ap-name> mesh cac callpath
```

| Depth | AP Name | Slot | Radio | Call |
|-------|------------------|------|-----------|------|
| 1 | APA023.9FA9.D920 | 0 | 802.11b/g | 2 |
| | | 1 | 802.11a | 0 |
| 2 | AP380E.4DBF.C80C | 0 | 802.11b/g | 0 |
| | | 1 | 802.11a | 2 |
| 2 | AP380E.4DBF.C816 | 0 | 802.11b/g | 0 |
| | | 1 | 802.11a | 0 |
| 2 | APA023.9FA9.B702 | 0 | 802.11b/g | 0 |
| | | 1 | 802.11a | 0 |

show ap mesh cac rejected

To view the number of rejected calls on access as well as backhaul for a given AP and its Mesh tree, use **show ap mesh cac rejected** command.

```
show ap ap-name mesh cac rejected
```

Syntax Description

ap-name Name of the access point.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines**Example**

This example shows how to display the number of rejected calls on access as well as backhaul for a given AP and its Mesh tree:

```
Device# show ap <ap-name> mesh cac rejected
```

show ap monitor-mode summary

To display the current channel-optimized monitor mode settings, use the **show ap monitor-mode summary** command.

show ap monitor-mode summary

| | |
|---------------------------|---|
| Syntax Description | This command has no keywords and arguments. |
|---------------------------|---|

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

| | |
|----------------------|------------------|
| Command Modes | Any command mode |
|----------------------|------------------|

| Command History | Release | Modification |
|------------------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to display current channel-optimized monitor mode settings:

```
Device# show ap monitor-mode summary
```

```
AP Name Ethernet MAC      Status   Scanning Channel List
-----
AP_004  xx:xx:xx:xx:xx:xx Tracking 1,6,11, 4
```

show ap multicast mom (multicast over multicast)

To confirm if the APs receive multicast to multicast (mom) traffic sent by the controller, using CAPWAP multicast group, use the **show ap multicast mom** command.

| Syntax Description | This command has no keywords and arguments. | | | | |
|-----------------------------|---|---------|--------------|-----------------------------|------------------------------|
| Command Default | None | | | | |
| Command Modes | Privileged EXEC | | | | |
| Command History | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Amsterdam 17.2</td> <td>This command was introduced.</td> </tr> </tbody> </table> | Release | Modification | Cisco IOS XE Amsterdam 17.2 | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE Amsterdam 17.2 | This command was introduced. | | | | |

This example shows how to confirm if the APs receive multicast to multicast traffic sent by the controller using CAPWAP multicast group:

Device# **show ap multicast mom**

| AP Name | MOM-IP | TYPE | MOM- | STATUS |
|------------------------|--------|------|------|--------|
| SS-E-1 | IPv4 | | | Up |
| SS-E-2 | IPv4 | | | Up |
| 9130E-r3-sw2-g1012 | IPv4 | | | Up |
| 9115i-r3-sw2-te1-0-38 | IPv4 | | | Up |
| AP9120-r3-sw3-Gi1-0-46 | IPv4 | | | Up |
| ap3800i-r2-sw1-te2-0-2 | IPv4 | | | Up |

show ap name *ap-name* neighbor summary

To view the summary of AP neighbor information, use the **show ap name** *ap-name* **neighbor summary**

show ap name *ap-name* **neighbor summary**

| | |
|---------------------------|--|
| Syntax Description | <i>ap-name</i> Specifies the name of the AP whose neighbor summary is displayed. |
|---------------------------|--|

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

| | |
|----------------------|--------------------|
| Command Modes | Privileged EXEC(#) |
|----------------------|--------------------|

| | | |
|------------------------|-------------------------------|------------------------------|
| Command History | Release | Modification |
| | Cisco IOS XE Amsterdam 17.2.1 | This command was introduced. |

Example

This example shows how to display the AP neighbor information:

```
Device#show ap name APXXXX.6DXX.59XX neighbor summary
```

| BSSID | Channel SSID | Channel-width | Slot | RSSI | Neighbour | Last-Heard |
|----------------------------|-----------------------|---------------|------|------|-----------|------------|
| 0008.2f1c.8040 18:25:14 | 1 aprusty-un-dot1x | 20 Mhz | 0 | -39 | FALSE | 03/17/2020 |
| 0008.2f1c.8041 18:25:14 | 1 aprusty-sim-11 | 20 Mhz | 0 | -39 | FALSE | 03/17/2020 |
| 0008.2f1c.8042 18:25:14 | 1 one-ph | 20 Mhz | 0 | -39 | FALSE | 03/17/2020 |
| 0008.2f1c.8044 18:25:14 | 1 aprusty-test | 20 Mhz | 0 | -38 | FALSE | 03/17/2020 |
| 0008.3296.f340 10:39:27 | 11 ewlc-ap-dot1x | 20 Mhz | 0 | -51 | FALSE | 03/18/2020 |
| 0008.3296.f341 10:39:27 | 11 vewlc_small_psk | 20 Mhz | 0 | -49 | FALSE | 03/18/2020 |
| 002a.1022.d950 18:25:14 | 1 ewlc-ap-dot1x | 20 Mhz | 0 | -57 | FALSE | 03/17/2020 |
| 002a.105c.bfd0 18:25:14 | 1 ewlc-ap-dot1x | 20 Mhz | 0 | -36 | FALSE | 03/17/2020 |
| 002a.105c.bfd1 18:25:14 | 1 vewlc_small_psk | 20 Mhz | 0 | -37 | FALSE | 03/17/2020 |
| 002c.c864.76d0 10:37:37 | 11 rajwlan | 20 Mhz | 0 | -61 | FALSE | 03/18/2020 |
| BSSID | Channel SSID | Channel-width | Slot | RSSI | Neighbour | Last-Heard |
| 002c.c8de.59e0 18:25:14 | 1 WQ | 20 Mhz | 0 | -48 | FALSE | 03/17/2020 |
| 002c.c8de.5d80 10:39:27 | 11 ewlc-ap-dot1x | 20 Mhz | 0 | -54 | FALSE | 03/18/2020 |
| 002c.c8de.5d81 10:39:27 | 11 vewlc_small_psk | 20 Mhz | 0 | -55 | FALSE | 03/18/2020 |

| | | | | | | |
|----------------------------|----|--------|---|-----|-------|------------|
| 002c.c8de.7260 10:39:27 | 11 | 20 Mhz | 0 | -53 | FALSE | 03/18/2020 |
| 002c.c8de.7261 10:39:27 | 11 | 20 Mhz | 0 | -54 | FALSE | 03/18/2020 |
| 005d.7390.e1e0 18:25:14 | 1 | 20 Mhz | 0 | -54 | FALSE | 03/17/2020 |
| 006b.f114.95a0 18:25:14 | 1 | 20 Mhz | 0 | -60 | FALSE | 03/17/2020 |
| 006b.f114.b0e0 18:25:14 | 1 | 20 Mhz | 0 | -46 | FALSE | 03/17/2020 |
| 006c.bc61.2340 18:24:44 | 1 | 20 Mhz | 0 | -63 | FALSE | 03/17/2020 |
| 006c.bc72.5ce0 10:39:17 | 11 | 20 Mhz | 0 | -58 | FALSE | 03/18/2020 |

show ap name afc detail

To view detailed information about the Automated Frequency Coordination (AFC) system, use the **show ap name afc detail** command.

show ap name *ap-name* **afc detail**

| | |
|---------------------------|--------------------------------------|
| Syntax Description | <i>ap-name</i> Name of the Cisco AP. |
|---------------------------|--------------------------------------|

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

| | |
|----------------------|---------------------|
| Command Modes | Privileged EXEC (#) |
|----------------------|---------------------|

| | | |
|------------------------|----------------------|------------------------------|
| Command History | Release | Modification |
| | Cisco IOS XE 17.13.1 | This command was introduced. |

Examples

The following example shows how to view detailed information about the AFC system:

```
Device# show ap name AP687D.B45C.17AC afc detail
```

```
AFC event history
```

| Timestamp | Event | AFC Status | Context |
|----------------------------|---|------------|-------------|
| 08/07/2023 16:07:01.244077 | AFC_EVT_REQ_RESP_RECEIVED | Active | ReqId |
| 12195125900336565037 | Response code: 0; SUCCESS | | |
| 08/07/2023 16:06:55.491957 | AFC_EVT_REQ_SENT | Inactive | ReqId |
| 12195125900336565037 | Sent to AFC System | | |
| 08/07/2023 16:06:51.823938 | AFC_EVT_REQ_QUEUED | Inactive | AFC request |
| | queued: immediate scheduling | | |
| 08/07/2023 15:28:54.608117 | AFC_EVT_REQ_INACTIVE | Inactive | No location |
| | information available; No height information available; | | |

show ap name afc geolocation

To view the geolocation information about the Automated Frequency Coordination (AFC) system of a Cisco AP, use the **show ap name afc geolocation** command.

show ap name *ap-name* afc geolocation

Syntax Description

ap-name Name of the Cisco AP.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

| Release | Modification |
|----------------------|------------------------------|
| Cisco IOS XE 17.13.1 | This command was introduced. |

Examples

The following example shows how to view the geolocation information of the AFC system of a Cisco AP:

```
Device# show ap name AP687D.B45C.17AC afc geolocation
Location type           : Ellipse
Center ellipse - longitude : -73.977769
Center ellipse - latitude  : 40.760168
Ellipse major-axis (meters) : 8
Ellipse minor-axis (meters) : 8
Ellipse orientation      : 2.5
Height (meters)         : 129
Uncertainty (meters)    : 3
```

show ap name afc response

To see the response from the Automated Frequency Coordination (AFC) system for a service request from an AP, use the **show ap name afc response** command.

show ap name *ap-name* **afc response**

| Syntax Description | <i>ap-name</i> Name of the Cisco AP. | | | | |
|---------------------------|--|---------|--------------|----------------------|------------------------------|
| Command Default | None | | | | |
| Command Modes | Privileged EXEC (#) | | | | |
| Command History | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 17.13.1</td> <td>This command was introduced.</td> </tr> </tbody> </table> | Release | Modification | Cisco IOS XE 17.13.1 | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE 17.13.1 | This command was introduced. | | | | |

Examples

The following example shows how to receive the response information received from the AFC system:

```
Device# show ap name AP687D.B45C.17AC afc response
AP name           : AP687D.B45C.17AC
AP MAC Address    : 687d.b45f.1af0
Response Code     : SUCCESS
Request ID        : 2
Expire Time       : 11/14/2021 21:56:30
Last Rcvd Time   : 11/14/2021 17:56:29
Global Operating Class : 131
Channel Cfi / Max Eirp :
1      / 36.000000
5      / 33.668693
9      / 36.000000
13     / 36.000000
17     / 35.223532
21     / 36.000000
25     / 36.000000
29     / 36.000000
.
.
.
```


show ap name auto-rf

To display the auto-RF settings for a Cisco lightweight access point, use the **show ap name auto-rf** command.

```
show ap name ap-name auto-rf dot11 {24ghz | 5ghz | dual-band}
```

| Syntax Description | <i>ap-name</i> | Name of the Cisco lightweight access point. |
|--------------------|--------------------------------|---|
| | 24ghz | Displays the 2.4 GHz band. |
| | 5ghz | Displays the 5 GHz band. |
| | dual-band | Displays dual band. |
| Command Default | None | |
| Command Modes | Privileged EXEC. | |
| Command History | Release | Modification |
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to display auto-RF information for an access point:

```
Device# show ap name AP01 auto-rf dot11 24ghz

Number of Slots                : 2
AP Name                        : TSIM_AP-1
MAC Address                    : 0000.2000.02f0
Slot ID                        : 0
Radio Type                     : 802.11b/g
Subband Type                   : All

Noise Information
  Noise Profile                : Failed
  Channel 1                    : 24 dBm
  Channel 2                    : 48 dBm
  Channel 3                    : 72 dBm
  Channel 4                    : 96 dBm
  Channel 5                    : 120 dBm
  Channel 6                    : -112 dBm
  Channel 7                    : -88 dBm
  Channel 8                    : -64 dBm
  Channel 9                    : -40 dBm
  Channel 10                   : -16 dBm
  Channel 11                   : 8 dBm

Interference Information
  Interference Profile         : Passed
  Channel 1                    : -128 dBm @ 0% busy
  Channel 2                    : -71 dBm @ 1% busy
  Channel 3                    : -72 dBm @ 1% busy
  Channel 4                    : -73 dBm @ 2% busy
  Channel 5                    : -74 dBm @ 3% busy
  Channel 6                    : -75 dBm @ 4% busy
  Channel 7                    : -76 dBm @ 5% busy
```

show ap name auto-rf

```

Channel 8 : -77 dBm @ 5% busy
Channel 9 : -78 dBm @ 6% busy
Channel 10 : -79 dBm @ 7% busy
Channel 11 : -80 dBm @ 8% busy

Rogue Histogram (20/40_ABOVE/40_BELOW)
Channel 36 : 27/ 4/ 0
Channel 40 : 13/ 0/ 0
Channel 44 : 5/ 0/ 0
Channel 48 : 6/ 0/ 1
Channel 52 : 4/ 0/ 0
Channel 56 : 5/ 0/ 0
Channel 60 : 1/ 3/ 0
Channel 64 : 3/ 0/ 0
Channel 100 : 0/ 0/ 0
Channel 104 : 0/ 0/ 0
Channel 108 : 0/ 1/ 0

Load Information
Load Profile : Passed
Receive Utilization : 10%
Transmit Utilization : 20%
Channel Utilization : 50%
Attached Clients : 0 clients

Coverage Information
Coverage Profile : Passed
Failed Clients : 0 clients

Client Signal Strengths
RSSI -100 dBm : 0 clients
RSSI -92 dBm : 0 clients
RSSI -84 dBm : 0 clients
RSSI -76 dBm : 0 clients
RSSI -68 dBm : 0 clients
RSSI -60 dBm : 0 clients
RSSI -52 dBm : 0 clients

Client Signal to Noise Ratios
SNR 0 dB : 0 clients
SNR 5 dB : 0 clients
SNR 10 dB : 0 clients
SNR 15 dB : 0 clients
SNR 20 dB : 0 clients
SNR 25 dB : 0 clients
SNR 30 dB : 0 clients
SNR 35 dB : 0 clients
SNR 40 dB : 0 clients
SNR 45 dB : 0 clients

Nearby APs
AP 0000.2000.0300 slot 0 : -68 dBm on 11 (10.10.10.1)
AP 0000.2000.0400 slot 0 : -68 dBm on 11 (10.10.10.1)
AP 0000.2000.0600 slot 0 : -68 dBm on 11 (10.10.10.1)

Radar Information

Channel Assignment Information
Current Channel Average Energy : 0 dBm
Previous Channel Average Energy : 0 dBm
Channel Change Count : 0
Last Channel Change Time : Wed Oct 17 08:13:36 2012
Recommended Best Channel : 11

```

RF Parameter Recommendations

| | |
|-------------------------|--------|
| Power Level | : 1 |
| RTS/CTS Threshold | : 2347 |
| Fragmentation Threshold | : 2346 |
| Antenna Pattern | : 0 |

Persistent Interference Devices

show ap name ble detail

To display BLE management details, use the **show ap name ble detail** command.

show ap name *ap-name* **ble detail**

| Syntax Description | <i>ap-name</i> Specifies the name of the AP. | | | | |
|-------------------------------|---|---------|--------------|-------------------------------|------------------------------|
| Command Default | None | | | | |
| Command Modes | Privileged EXEC (#) | | | | |
| Command History | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Amsterdam 17.3.1</td> <td>This command was introduced.</td> </tr> </tbody> </table> | Release | Modification | Cisco IOS XE Amsterdam 17.3.1 | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE Amsterdam 17.3.1 | This command was introduced. | | | | |
| Usage Guidelines | None | | | | |

Example

The following example shows how to display the BLE management details:

```
Device(config)# show ap name ap-name ble detail
```

show ap name cablemodem

To see cable modem information of an AP, use the **show ap name *ap-name* cablemodem** command.

```
show ap name ap-name cablemodem [chassis {chassis-number | active | standby} R0]
```

Syntax Description

| | |
|-----------------------|---|
| <i>ap-name</i> | Name of the AP. |
| <i>chassis-number</i> | Enter the chassis number as either 1 or 2. |
| active R0 | Active instance of the AP filters in Route-processor slot 0. |
| standby R0 | Standby instance of the AP filters in Route-processor slot 0. |

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Examples

The following example shows how to see cable modem information of an AP:

```
Device# show ap name my-ap cablemodem
```

show ap name config

To display common information and Ethernet VLAN tagging information for a specific Cisco lightweight access point, use the **show ap name config** command.

```
show ap name ap-name config {ethernet | general}
```

| Syntax Description | <i>ap-name</i> Name of the Cisco lightweight access point. | | | | |
|--------------------------------|--|---------|--------------|--------------------------------|------------------------------|
| | ethernet Displays Ethernet tagging configuration information for an access point. | | | | |
| | general Displays common information for an access point. | | | | |
| Command Default | None | | | | |
| Command Modes | Any command mode | | | | |
| Command History | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.10.1</td> <td>This command was introduced.</td> </tr> </tbody> </table> | Release | Modification | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. | | | | |

This example shows how to display Ethernet tagging information for an access point:

```
Device# show ap name AP01 config ethernet
```

```
VLAN Tagging Information for AP01
```

This example shows how to display common information for an access point:

```
Device# show ap name AP01 config general
```

```
Cisco AP Name : AP01
Cisco AP Identifier : 5
Country Code : US - United States
Regulatory Domain Allowed by Country : 802.11bg:-A 802.11a:-A
AP Country Code : US - United States
AP Regulatory Domain : Unconfigured
Switch Port Number : Tel1/0/1
MAC Address : 0000.2000.02f0
IP Address Configuration : Static IP assigned
IP Address : 10.10.10.12
IP Netmask : 255.255.0.0
Gateway IP Address : 10.10.10.1
Fallback IP Address Being Used : 10.10.10.12
Domain : Cisco
Name Server : 0.0.0.0
CAPWAP Path MTU : 1485
Telnet State : Enabled
SSH State : Disabled
Cisco AP Location : sanjose
Cisco AP Group Name : default-group
Primary Cisco Controller Name : CAPWAP Controller
Primary Cisco Controller IP Address : 10.10.10.1
Secondary Cisco Controller Name :
Secondary Cisco Controller IP Address : Not Configured
```

```
Tertiary Cisco Controller Name           :
Tertiary Cisco Controller IP Address    : Not Configured
Administrative State                     : Enabled
Operation State                          : Registered
AP Mode                                  : Local
AP Submode                               : Not Configured
Remote AP Debug                          : Disabled
Logging Trap Severity Level              : informational
Software Version                         : 7.4.0.5
Boot Version                             : 7.4.0.5
Stats Reporting Period                   : 180
LED State                                 : Enabled
PoE Pre-Standard Switch                  : Disabled
PoE Power Injector MAC Address           : Disabled
Power Type/Mode                          : Power Injector/Normal Mode
Number of Slots                          : 2
AP Model                                  : 1140AG
AP Image                                  : C1140-K9W8-M
IOS Version                               :
Reset Button                             :
AP Serial Number                         : SIM1140K001
AP Certificate Type                      : Manufacture Installed
Management Frame Protection Validation   : Disabled
AP User Mode                             : Customized
AP User Name                             : cisco
AP 802.1X User Mode                      : Not Configured
AP 802.1X User Name                     : Not Configured
Cisco AP System Logging Host             : 255.255.255.255
AP Up Time                               : 15 days 16 hours 19 minutes 57
seconds
AP CAPWAP Up Time                       : 4 minutes 56 seconds
Join Date and Time                      : 10/18/2012 04:48:56
Join Taken Time                         : 15 days 16 hours 15 minutes 0
seconds
Join Priority                            : 1
Ethernet Port Duplex                    : Auto
Ethernet Port Speed                     : Auto
AP Link Latency                         : Disabled
Rogue Detection                         : Disabled
AP TCP MSS Adjust                       : Disabled
AP TCP MSS Size                         : 6146
```

show ap name config dot11 6ghz

To view the 802.11 parameter configuration of a Cisco AP, use the **show ap name config dot11 6ghz** command.

show ap name *ap-name* **config dot11 6ghz**

| Syntax Description | <i>ap-name</i> Name of the Cisco AP. | | | | |
|---------------------------|--|---------|--------------|----------------------|------------------------------|
| Command Default | None | | | | |
| Command Modes | Privileged EXEC (#) | | | | |
| Command History | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 17.13.1</td> <td>This command was introduced.</td> </tr> </tbody> </table> | Release | Modification | Cisco IOS XE 17.13.1 | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE 17.13.1 | This command was introduced. | | | | |

Examples

The following example shows how to view the 802.11 parameter configuration of a Cisco AP:

```
Device# show ap name AP687D.B45C.17AC config dot11 6ghz
AP 6GHZ Power Mode           : Low Power Indoor
Low Power Indoor Capable     : Yes
Standard Power Capable       : Yes
```


show ap name config slot

To display the configuration of a Cisco AP and also display the common information for a slot, use the **show ap name config slot** command.

```
show ap name Cisco-ap-name slot 0-3
```

| | | |
|---------------------------|--------------------------------|-------------------------------------|
| Syntax Description | <i>Cisco-ap-name</i> | Specifies the name of the Cisco AP. |
| | <i>0-3</i> | Specifies the slot ID. |
| Command Default | None | |
| Command Modes | Any command mode | |
| Command History | Release | Modification |
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

Example

This example shows how to display common information for a slot in an access point:

```
Device# show ap name Cisco-ap-name config slot 3
```

show ap name config ethernet

To see Ethernet related configuration information of an AP, use the **show ap name *ap-name* config ethernet** command.

show ap name *ap-name* config ethernet [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

| Syntax Description | |
|-----------------------|---|
| <i>ap-name</i> | Name of the AP. |
| <i>chassis-number</i> | Enter the chassis number as either 1 or 2. |
| active R0 | Active instance of the AP filters in Route-processor slot 0. |
| standby R0 | Standby instance of the AP filters in Route-processor slot 0. |

Command Default None

Command Modes Privileged EXEC

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

Examples

The following example shows how to see Ethernet related configuration information of an AP:

```
Device# show ap name my-ap config ethernet
```

show ap name dot11

To display 802.11a or 802.11b configuration information that corresponds to specific Cisco lightweight access points, use the **show ap name dot11** command.

```
show ap name ap-name dot11 { 24ghz | 5ghz | 6ghz } { ccx | cdp | profile | service-policy
output | tsm { all client-mac } }
```

| Syntax | Description |
|------------------------------|---|
| <i>ap-name</i> | Name of the Cisco lightweight access point. |
| 24ghz | Displays the 2.4-GHz band. |
| 5ghz | Displays the 5-GHz band. |
| 6ghz | Displays the 6-GHz band. |
| ccx | Displays the Cisco Client eXtensions (CCX) radio management status information. |
| cdp | Displays Cisco Discovery Protocol (CDP) information. |
| profile | Displays configuration and statistics of 802.11 profiling. |
| service-policy output | Displays downstream service policy information. |
| tsm | Displays 802.11 traffic stream metrics statistics. |
| all | Displays the list of all access points to which the client has associations. |
| <i>client-mac</i> | MAC address of the client. |
| SI | Displays the SI configurations. |
| airtime-fairness | Displays the stats of 24Ghz or 5Ghz or 6-GHz airtime-fairness. |
| call-control | Displays the call control information. |
| radio-reset | Displays radio-reset. |
| slot | Displays slot information. |
| voice | Displays voice information. |

Command Default None

Command Modes Any command mode

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

This example shows how to display the service policy that is associated with the access point:

```
Device# show ap name test-ap dot11 24ghz service-policy output

Policy Name   : test-ap1
Policy State  : Installed
```

This example shows how to display the CCX RRM 802.11 configuration for a specific access point:

```
Device# show ap name AP01 dot11 24ghz ccx
```

This example show how to display CDP information for a specific access point:

```
Device# show ap name AP01 dot11 24ghz cdp

AP Name                AP CDP State
-----
AP03                    Disabled
```

This example show how to display the configuration and statistics of 802.11b profiling for a specific access point:

```
Device# show ap name AP01 dot11 24ghz profile

802.11b Cisco AP performance profile mode      : GLOBAL
802.11b Cisco AP Interference threshold       : 10 %
802.11b Cisco AP noise threshold              : -70 dBm
802.11b Cisco AP RF utilization threshold     : 80 %
802.11b Cisco AP throughput threshold        : 1000000 bps
802.11b Cisco AP clients threshold           : 12 clients
```

This example show how to display downstream service policy information for a specific access point:

```
Device# show ap name AP01 dot11 24ghz service-policy output

Policy Name   : def-11gn
Policy State  : Installed
```

This example show how to display the traffic stream configuration for all clients that correspond to a specific access point:

```
Device# show ap name AP01 dot11 24ghz tsm all
```

show ap name dot11 6ghz power-mode

To view the power-mode of a Cisco AP, use the **show ap name dot11 6ghz power-mode** command.

```
show ap name ap-name dot11 6ghz power-mode
```

| Syntax Description | <i>ap-name</i> Name of the Cisco AP. | | | | |
|---------------------------|--|---------|--------------|----------------------|------------------------------|
| Command Default | None | | | | |
| Command Modes | Privileged EXEC (#) | | | | |
| Command History | <table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>Cisco IOS XE 17.13.1</td><td>This command was introduced.</td></tr></tbody></table> | Release | Modification | Cisco IOS XE 17.13.1 | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE 17.13.1 | This command was introduced. | | | | |

Examples

The following example shows how to view the power-mode of a Cisco AP:

```
Device# show ap name AP687D.B45C.17AC dot11 6ghz power-mode
i Power mode
Standard-power mode: Allowed
```

show ap name environment

To see the AP environment information of an AP, use the **show ap name *ap-name* environment** command.

show ap name *ap-name* environment [chassis {*chassis-number* | active | standby} R0]

Syntax Description

| | |
|-----------------------|---|
| <i>ap-name</i> | Name of the AP. |
| <i>chassis-number</i> | Enter the chassis number as either 1 or 2. |
| active R0 | Active instance of the AP filters in Route-processor slot 0. |
| standby R0 | Standby instance of the AP filters in Route-processor slot 0. |

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Examples

The following example shows how to see the AP environment information of an AP:

```
Device# show ap name my-ap environment
```

show ap name gps location

To see the GPS location of the AP, use the **show ap name gps location** command.

```
show ap name ap-name gps location [ {chassis-number | active | standby} R0
```

| Syntax Description | |
|-----------------------|---|
| <i>ap-name</i> | Name of the Access Point |
| gps | See the GPS information of a Cisco AP |
| location | Shows the Mesh linktest data |
| <i>chassis-number</i> | Enter the chassis number as either 1 or 2. |
| active R0 | Active instance of the active AP filters in Route-processor slot 0. |
| standby R0 | Standby instance of the configuration in Route-processor slot 0. |

Command Default None

Command Modes Privileged EXEC

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

Examples

The following example shows how to see the GPS location of an AP:

```
Device# show ap name mesh-profile-name gps location
```

show ap name grpc detail

To display the detailed status of gRPC channel from AP to Cisco DNA, use the **show ap name grpc detail** command.

show ap name *ap-name* **grpc detail**

| Syntax Description | <i>ap-name</i> Specifies the name of the AP. | | | | |
|-------------------------------|---|---------|--------------|-------------------------------|------------------------------|
| Command Default | None | | | | |
| Command Modes | Privileged EXEC (#) | | | | |
| Command History | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Amsterdam 17.3.1</td> <td>This command was introduced.</td> </tr> </tbody> </table> | Release | Modification | Cisco IOS XE Amsterdam 17.3.1 | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE Amsterdam 17.3.1 | This command was introduced. | | | | |
| Usage Guidelines | None | | | | |

Example

The following example shows how to display the detailed status of gRPC channel from AP to Cisco DNA:

```
Device(config)# show ap name APXXXX.BXXX.FXXX grpc detail
```


show ap name hyperlocation

To view a summary or detailed information about the hyperlocation configuration for an access point (AP), use the **show ap name hyperlocation** command.

show ap name *ap-name* hyperlocation ble-beacon

| Syntax Description | | |
|--------------------|----------------------|---|
| | <i>ap-name</i> | Access point name. |
| | hyperlocation | Displays AP hyperlocation information. |
| | ble-beacon | Displays BLE beacon configuration of an AP. |

Command Modes Privileged EXEC (#)

| Command History | Release | Modification |
|-----------------|----------------------------|------------------------------|
| | Cisco IOS XE Denali 16.3.1 | This command was introduced. |

Example

This example shows how to view the BLE beacon configuration of an AP:

```
Device# show ap name test-ap hyperlocation ble-beacon
```

```
ID Major Minor TX Power(dBm)
-----
0 0 0 0
1 0 0 0
2 0 0 0
3 0 0 0
```

show ap name mesh backhaul

To see mesh backhaul statistics of an AP, use the **show ap name *ap-name* mesh backhaul** command.

show ap name *ap-name* mesh backhaul [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

Syntax Description

chassis-number Enter the chassis number as either 1 or 2.

active R0 Active instance of the AP filters in Route-processor slot 0.

standby R0 Standby instance of the AP filters in Route-processor slot 0.

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Examples

The following example shows how to see mesh backhaul statistics of an AP:

```
Device# show ap name mymeshap mesh backhaul
```

show ap name mesh bhrate

To see mesh backhaul data rate for an AP, use the **show ap name *ap-name* mesh bhrate** command.

show ap name *ap-name* mesh bhrate [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

| | |
|-----------------------|---|
| <i>ap-name</i> | Name of the AP. |
| <i>chassis-number</i> | Enter the chassis number as either 1 or 2. |
| active R0 | Active instance of the AP filters in Route-processor slot 0. |
| standby R0 | Standby instance of the AP filters in Route-processor slot 0. |

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Examples

The following example shows how to see mesh backhaul data rate for an AP:

```
Device# show ap name mymeshap mesh bhrate
```

show ap name mesh linktest

To see the mesh linktest data, use the **show ap name mesh linktest data** command.

show ap name *ap-name* **mesh linktest data** *dest-mac* [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

| Syntax Description | |
|-----------------------|--|
| <i>ap-name</i> | Name of the Access Point |
| linktest | Shows the Mesh linktest |
| data | Shows the Mesh linktest data |
| <i>dest-mac</i> | Enter the AP MAC address. |
| <i>chassis-number</i> | Enter the chassis number as either 1 or 2. |
| active R0 | Active instance of the configuration in Route-processor slot 0. |
| standby R0 | Standby instance of the configuration in Route-processor slot 0. |

Command Default None

Command Modes Privileged EXEC

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

Examples

The following example shows how to see the mesh linktest data of an AP:

```
Device# show ap name mesh-profile-name mesh linktest data 83-88-15-0C-83-72
```

show ap name mesh neighbor detail

To see detailed information about a neighbor of a mesh AP, use the **show ap name *ap-name* mesh neighbor detail** command.

show ap name *ap-name* mesh neighbor detail [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

| Syntax Description | |
|-----------------------|---|
| <i>ap-name</i> | Name of the AP. |
| <i>chassis-number</i> | Enter the chassis number as either 1 or 2. |
| active R0 | Active instance of the AP filters in Route-processor slot 0. |
| standby R0 | Standby instance of the AP filters in Route-processor slot 0. |

Command Default None

Command Modes Privileged EXEC

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

Examples

The following example shows how to see detailed information about a neighbor of a mesh AP:

```
Device# show ap name mymeshap mesh neighbor detail
```

show ap name mesh neighbor detail

To see detailed information about a neighbor of a mesh AP, use the **show ap name *ap-name* mesh neighbor detail** command.

show ap name *ap-name* mesh neighbor detail [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

| Syntax Description | |
|-----------------------|---|
| <i>ap-name</i> | Name of the AP. |
| <i>chassis-number</i> | Enter the chassis number as either 1 or 2. |
| active R0 | Active instance of the AP filters in Route-processor slot 0. |
| standby R0 | Standby instance of the AP filters in Route-processor slot 0. |

Command Default None

Command Modes Privileged EXEC

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

Examples

The following example shows how to see detailed information about a neighbor of a mesh AP:

```
Device# show ap name mymeshap mesh neighbor detail
```

show ap name mesh path

To see information about the mesh AP's path, use the **show ap name *ap-name* mesh path** command.

show ap name *ap-name* mesh path [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

Syntax Description

chassis-number Enter the chassis number as either 1 or 2.

active R0 Active instance of the AP filters in Route-processor slot 0.

standby R0 Standby instance of the AP filters in Route-processor slot 0.

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Examples

The following example shows how to see information about the mesh AP's path:

```
Device# show ap name mymeshap mesh path
```

show ap name mesh stats

To see mesh statistics, use the **show ap name *ap-name* mesh stats** command.

```
show ap name ap-name [{packet error | queue | security}]
```

Syntax Description

| | |
|-----------------------|---|
| <i>ap-name</i> | Name of the AP. |
| packet error | Mesh packet error statistics. |
| queue | Mesh queue statistics. |
| security | Mesh security statistics. |
| <i>chassis-number</i> | Enter the chassis number as either 1 or 2. |
| active R0 | Active instance of the AP filters in Route-processor slot 0. |
| standby R0 | Standby instance of the AP filters in Route-processor slot 0. |

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Examples

The following example shows how to see mesh statistics:

```
Device# show ap name mymeshap mesh stats
```


show ap name tunnel eogre events

To display the Ethernet over GRE (EoGRE) events on an AP, use the **show ap name tunnel eogre events** command.

show ap name *ap-name* **tunnel eogre events**

| | |
|---------------------------|-------------------------|
| Syntax Description | <i>ap-name</i> AP name. |
|---------------------------|-------------------------|

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

| | |
|----------------------|---------------------|
| Command Modes | Privileged EXEC (#) |
|----------------------|---------------------|

| Command History | Release | Modification |
|------------------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.11.1 | This command was introduced. |

Example

This example shows how to display the EoGRE tunnel events on an AP:

```
Device# show ap name ap1 tunnel eogre events

AP 80e8.6fd4.9520 Event history
Timestamp          #Times  Event                               RC Context
-----
02/18/2019 23:50:26.341 6      IAPP_STATS                          0 GW Tunnel2 uptime:0s
02/18/2019 23:49:40.222 2      CLIENT_JOIN                          0 74da.3828.88b0, (eogre_domain/2121)
02/18/2019 23:48:43.549 1      CLIENT_LEAVE                         0 74da.3828.88b0, (eogre_domain/2121)
02/18/2019 23:47:33.127 1      DOMAIN_STATUS                       0 eogre_domain Active GW: Tunnel1
02/18/2019 23:47:33.124 4      AP_TUNNEL_STATUS                    0 Tunnel2 Dn
02/18/2019 23:47:33.124 1      MSG_CLIENT_DEL                      0 GW Tunnel2 (IP: 9.51.1.12)
02/18/2019 23:47:33.124 2      TUNNEL_ADD                          0 GW Tunnel2
02/18/2019 23:47:33.120 3      MSG_CLIENT_DEL_PD                   0 GW Tunnel1 (IP: 9.51.1.11)
02/18/2019 23:47:31.763 2      AP_DOMAIN_PUSH                      0 Delete:eogre_domain_set, 0 GWs
02/18/2019 23:47:31.753 4      AP_VAP_PUSH                         0 profile:'eogre_tunnel',
wlan:pyats_eogre
```

show ap name tunnel eogre domain detailed

To display the detailed information of the Ethernet over GRE (EoGRE) tunnel domain status on an AP, use the **show ap name tunnel eogre domain detailed** command.

show ap name *ap-name* **tunnel eogre domain detailed** *domain-name*

| Syntax Description | | |
|--------------------|--------------------|--------------------|
| | <i>ap-name</i> | AP name. |
| | <i>domain-name</i> | EoGRE domain name. |

Command Default None

Command Modes Privileged EXEC (#)

| Command History | Release | Modification |
|-----------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.11.1 | This command was introduced. |

Example

This example shows how to display the detailed information of the EoGRE tunnel domain status on an AP:

```
Device# show ap name ap1 tunnel eogre domain detailed eogre_domain
```

```
Domain Name      : eogre_domain
Primary GW       : Tunnel1
Secondary GW     : Tunnel2
Active GW        : Tunnel1
Redundancy       : Non-Revertive
AdminState       : Up
```

show ap name tunnel eogre domain summary

To display the summary information of the Ethernet over GRE (EoGRE) tunnel domain on an AP, use the **show ap name tunnel eogre domain summary** command.

show ap name *ap-name* **tunnel eogre domain summary**

| | |
|---------------------------|---|
| Syntax Description | <i>ap-name</i> AP name. |
| Command Default | None |
| Command Modes | Privileged EXEC (#) |
| Command History | Release |
| | Modification |
| | Cisco IOS XE Gibraltar 16.11.1 This command was introduced. |

Example

This example shows how to display the summary information of the EoGRE tunnel domain on an AP:

```
Device# show ap name ap1 tunnel eogre domain summary
```

```
AP MAC           Domain           Active Gateway
-----
80e8.6fd4.9520  eogre_domain
```

show ap name tunnel eogre gateway detailed

To display the detailed information of the Ethernet over GRE (EoGRE) tunnel gateway status on an AP, use the **show ap name tunnel eogre gateway detailed** command.

show ap name *ap-name* **tunnel eogre gateway detailed** *gateway-name*

| | | |
|---------------------------|--------------------------------|------------------------------|
| Syntax Description | <i>ap-name</i> | AP name. |
| | <i>gateway-name</i> | EoGRE gateway name. |
| Command Default | None | |
| Command Modes | Privileged EXEC (#) | |
| Command History | Release | Modification |
| | Cisco IOS XE Gibraltar 16.11.1 | This command was introduced. |

Example

This example shows how to display the detailed information of the EoGRE tunnel gateway status on an AP:

```
Device# show ap name ap1 tunnel eogre gateway detailed Tunnel2
```

```
Gateway : Tunnel2
Mode    : IPv4
IP      : 9.51.1.12
State   : Down
MTU     : 0
AP MAC  : 80e8.6fd4.9520

Clients
Total Number of Wireless Clients      : 0
Traffic
Total Number of Received Packets     : 0
Total Number of Received Bytes       : 0
Total Number of Transmitted Packets   : 0
Total Number of Transmitted Bytes     : 0
Total Number of Lost Keepalive       : 151
```

show ap name tunnel eogre gateway summary

To display the summary information of the Ethernet over GRE (EoGRE) tunnel gateway on an AP, use the **show ap name tunnel eogre gateway summary** command.

show ap name *ap-name* **tunnel eogre gateway summary**

| Syntax Description | <i>ap-name</i> AP name. | | | | |
|--------------------------------|--|---------|--------------|--------------------------------|------------------------------|
| Command Default | None | | | | |
| Command Modes | Privileged EXEC (#) | | | | |
| Command History | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.11.1</td> <td>This command was introduced.</td> </tr> </tbody> </table> | Release | Modification | Cisco IOS XE Gibraltar 16.11.1 | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE Gibraltar 16.11.1 | This command was introduced. | | | | |

Example

This example shows how to display the summary information of the EoGRE tunnel gateway on an AP:

```
Device# show ap name ap1 tunnel eogre gateway summary
```

| AP MAC | Gateway | Type | IP | State | Clients |
|----------------|---------|------|-----------|-------|---------|
| 80e8.6fd4.9520 | Tunnel1 | IPv4 | 9.51.1.11 | Up | 1 |
| 80e8.6fd4.9520 | Tunnel2 | IPv4 | 9.51.1.12 | Down | 0 |

show ap name wlan

To display the Basic Service Set Identifier (BSSID) value for each WLAN defined on an access point and to display WLAN statistics, use the **show ap name wlan** command.

```
show ap name ap-name wlan {dot11 {24ghz | 5ghz} | statistic}
```

| Syntax Description | |
|--------------------|---|
| <i>ap-name</i> | Name of the Cisco lightweight access point. |
| dot11 | Displays 802.11 parameters. |
| 24ghz | Displays 802.11b network settings. |
| 5ghz | Displays 802.11a network settings. |
| statistic | Displays WLAN statistics. |

Command Default None

Command Modes Any command mode

| Command History | Release | Modification |
|-----------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to display BSSID information of an access point in an 802.11b network:

```
Device# show ap name AP01 wlan dot11 24ghz

Site Name                : default-group
Site Description         :

WLAN ID  Interface  BSSID
-----
1        default    00:00:20:00:02:00
12       default    00:00:20:00:02:0b
```

This example shows how to display WLAN statistics for an access point:

```
Device# show ap name AP01 wlan statistic

WLAN ID  : 1
WLAN Profile Name  : maria-open

EAP Id Request Msg Timeouts           : 0
EAP Id Request Msg Timeouts Failures  : 0
EAP Request Msg Timeouts               : 0
EAP Request Msg Timeouts Failures     : 0
EAP Key Msg Timeouts                   : 0
EAP Key Msg Timeouts Failures         : 0

WLAN ID  : 12
WLAN Profile Name  : 24
```

```
EAP Id Request Msg Timeouts           : 0
EAP Id Request Msg Timeouts Failures  : 0
EAP Request Msg Timeouts               : 0
EAP Request Msg Timeouts Failures     : 0
EAP Key Msg Timeouts                   : 0
EAP Key Msg Timeouts Failures         : 0
```

show ap name wlan vlan

To display the operational WLAN-VLAN mappings for each access point (AP), use the **show ap name wlan vlan** command.

show ap name *ap_name* **wlan vlan**

| | |
|---------------------------|---|
| Syntax Description | <i>ap_name</i> Name of the AP whose WLAN-VLAN mappings are to be displayed. |
|---------------------------|---|

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

| | |
|----------------------|---------------------|
| Command Modes | Privileged EXEC (#) |
|----------------------|---------------------|

| Command History | Release | Modification |
|------------------------|-------------------------------|------------------------------|
| | Cisco IOS XE Bengaluru 17.6.1 | This command was introduced. |

The following example shows the operational wlan vlan mappings for an AP:

```
Device# show ap name test wlan vlan
```

```
Policy tag mapping
```

| WLAN Profile Name | Name | Policy | VLAN | Flex Central Switching | IPv4 ACL | IPv6 ACL |
|-------------------|------------|--------|------|------------------------|----------|----------------|
| jey_cwa | pp-local-1 | | 46 | Enabled | jey_acl1 | Not Configured |
| swaguest | pp-local-1 | | 46 | Enabled | jey_acl1 | Not Configured |

show ap name ble detail

To view the CMX associated with an AP, use the **show ap name ble detail** command.

show ap name *ap-name* **ble detail**

Syntax Description

ap-name Specifies the name of the AP.

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

This example shows how to display the global values for BLE and BLE details for a specific AP:

```
Device# show ap name AP4001.7AB2.C39A ble detail
CMX IP: 9.9.71.100
```

```
-----
BLE administrative status: Up
BLE operational status: Up
Scanning interval: 10
```

| AP Name | Interface | Status |
|------------------|------------|--------|
| AP4001.7AB2.C39A | Integrated | Open |

show ap name temperature

To view the temperature information of an AP, use the **show ap name temperature** command.

show ap name *ap-name* **temperature**

| | |
|---------------------------|-------------------------|
| Syntax Description | <i>ap-name</i> AP name. |
|---------------------------|-------------------------|

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

| | |
|----------------------|---------------------|
| Command Modes | Privileged EXEC (#) |
|----------------------|---------------------|

| Command History | Release | Modification |
|------------------------|-------------------------------|------------------------------|
| | Cisco IOS XE Amsterdam 17.3.1 | This command was introduced. |

Examples

This example shows how to view the temperature information of an AP:

```
Device# show ap name ap-3702 temperature
```

show ap management-mode meraki capability summary

To display the Meraki management mode capable AP information summary, use the **show ap management-mode meraki capability summary**

show ap management-mode meraki capability summary

| Syntax Description | This command has no keywords or arguments. | | | | |
|-------------------------------|---|---------|--------------|-------------------------------|----------------------------|
| Command Default | None | | | | |
| Command Modes | Privileged EXEC(#) | | | | |
| Command History | <table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>Cisco IOS XE Cupertino 17.9.1</td><td>This command was modified.</td></tr></tbody></table> | Release | Modification | Cisco IOS XE Cupertino 17.9.1 | This command was modified. |
| Release | Modification | | | | |
| Cisco IOS XE Cupertino 17.9.1 | This command was modified. | | | | |

Example

This example show how to display the Meraki management mode capable AP information summary:

```
Device# show ap management-mode meraki capability summary
```

show ap management-mode meraki change summary

To display the summary of the AP management mode meraki changes, use the **show ap management-mode meraki change summary** command.

show ap management-mode meraki change summary

| | |
|---------------------------|--|
| Syntax Description | This command has no keywords or arguments. |
|---------------------------|--|

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

| | |
|----------------------|--------------------|
| Command Modes | Privileged EXEC(#) |
|----------------------|--------------------|

| Command History | Release | Modification |
|------------------------|-------------------------------|----------------------------|
| | Cisco IOS XE Cupertino 17.9.1 | This command was modified. |

Example

This example shows how to display the summary of the AP management mode meraki changes:

```
Device# show ap management-mode meraki change summary
```

show ap management-mode meraki failure summary

To display the Meraki management mode failure summary, use the **show ap management-mode meraki failure summary** command.

show ap management-mode meraki failure summary

| | | |
|---------------------------|--|----------------------------|
| Syntax Description | This command has no keywords or arguments. | |
| Command Default | None | |
| Command Modes | Privileged EXEC(#) | |
| Command History | Release | Modification |
| | Cisco IOS XE Cupertino 17.9.1 | This command was modified. |

Example

This example shows how to display the Meraki management mode failure summary:

```
Device# show ap management-mode meraki failure summary
```

show ap neighborhood

To view the AP neighborhood information, use the **show ap neighborhood** command.

show ap neighborhood *id* details

| | |
|---------------------------|---|
| Syntax Description | <i>id</i> Neighborhood ID. |
| | details Displays the neighborhood details. |

Command Default None

Command Modes Privileged EXEC (#)

| Command History | Release | Modification |
|------------------------|-----------------------------|------------------------------|
| | Cisco IOS XE Dublin 17.12.1 | This command was introduced. |

Examples

The following example shows how to view the AP neighborhood information:

```
Device# show ap neighborhood 0 details
```

```
NH-ID = Neighborhood ID
AREA-ID = Area ID of neighborhood
```

```
Number of APs: 1
```

| NH-ID | AREA-ID | WNCD instance | AP Name | Ethernet MAC |
|-------|------------|---------------|------------------|----------------|
| 0 | 0x00000000 | 0 | APA023.9FD8.EA22 | a023.9fd8.ea22 |

show ap neighborhood details

To view the AP neighborhood details, use the **show ap neighborhood details** command.

show ap neighborhood details

| | |
|---------------------------|--|
| Syntax Description | This command has no keywords or arguments. |
|---------------------------|--|

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

| | |
|----------------------|---------------------|
| Command Modes | Privileged EXEC (#) |
|----------------------|---------------------|

| Command History | Release | Modification |
|------------------------|-----------------------------|------------------------------|
| | Cisco IOS XE Dublin 17.12.1 | This command was introduced. |

Examples

The following example shows how to view the AP neighborhood details:

```
Device# show ap neighborhood details
```

```
NH-ID = Neighborhood ID
AREA-ID = Area ID of neighborhood
```

```
Number of APs: 4
```

| NH-ID | AREA-ID | WNCD instance | AP Name | Ethernet MAC |
|-------|------------|---------------|----------------------|----------------|
| 0 | 0x00000000 | 1 | EDU_BR_01_00_28_3702 | bc16.6509.bfcc |
| 1 | 0x00000000 | 0 | ci-glad-mdns-ap | 0cd0.f894.567c |
| 1 | 0x00000000 | 0 | EDU_VW_9120_1_2 | c4f7.d54c.f978 |
| 2 | 0x00000000 | 0 | ewlc-hc-tsim-30-1 | 00b9.3000.02f0 |

show ap neighborhood mac details

To view the AP neighborhood details using MAC address, use the **show ap neighborhood mac details** command.

show ap neighborhood mac *mac-address* **details**

| Syntax Description | |
|--------------------|--|
| <i>mac-address</i> | AP's MAC address. |
| details | Specifies the AP neighborhood details. |

Command Default None

Command Modes Privileged EXEC (#)

| Command History | Release | Modification |
|-----------------|-----------------------------|------------------------------|
| | Cisco IOS XE Dublin 17.12.1 | This command was introduced. |

Example

The following example shows how to view the AP neighborhood details using MAC address:

```
Device# show ap neighborhood mac 0aa8.89f0.0001 details
```

```
NH-ID = Neighborhood ID  
AREA-ID = Area ID of neighborhood
```

| AP Name | Ethernet MAC | Radio MAC | NH-ID | AREA-ID | WNCD instance |
|-----------------|----------------|----------------|-------|------------|---------------|
| AP6B8B4567-0001 | 0aa8.89f0.0001 | 0aa8.8900.0100 | 0 | 0x00000000 | 0 |

show ap neighborhood summary

To view the AP neighborhood summary, use the **show ap neighborhood summary** command.

show ap neighborhood summary

| | |
|---------------------------|--|
| Syntax Description | This command has no keywords or arguments. |
|---------------------------|--|

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

| | |
|----------------------|---------------------|
| Command Modes | Privileged EXEC (#) |
|----------------------|---------------------|

| Command History | Release | Modification |
|------------------------|-----------------------------|------------------------------|
| | Cisco IOS XE Dublin 17.12.1 | This command was introduced. |

Examples

The following example shows how to view the AP neighborhood summary:

```
Device# show ap neighborhood summary
```

```
NH-ID = Neighborhood ID
```

```
AREA-ID = Area ID of neighborhood
```

```
Total number of neighborhood: 5
```

```
Total number of algorithm iterations: 1
```

```
Ideal AP capacity per WNCD instance: 210
```

```
Total number of neighborhood area: 14
```

| NH-ID | AREA-ID | Process Name | Number of APs |
|-------|------------|--------------|---------------|
| 0 | 0x00000000 | WNCD_1 | 1 |
| 1 | 0x00000000 | WNCD_0 | 2 |
| 2 | 0x00000000 | WNCD_0 | 100 |
| 2 | 0x00000001 | WNCD_0 | 100 |
| 2 | 0x00000002 | WNCD_3 | 100 |
| 2 | 0x00000003 | WNCD_4 | 50 |
| 3 | 0x00000000 | WNCD_1 | 100 |
| 3 | 0x00000001 | WNCD_1 | 100 |
| 3 | 0x00000002 | WNCD_4 | 100 |
| 3 | 0x00000003 | WNCD_4 | 50 |
| 4 | 0x00000000 | WNCD_2 | 100 |
| 4 | 0x00000001 | WNCD_2 | 100 |
| 4 | 0x00000002 | WNCD_3 | 100 |
| 4 | 0x00000003 | WNCD_3 | 50 |

show ap profile

To see overall status of Hyperlocation for an AP profile, use the **show ap profile** command.

```
show ap profile profile-name {detailed | hyperlocation {ble-beacon | detail | summary}} [chassis
{chassis-number | active | standby} R0]
```

| Syntax Description | |
|-----------------------|---|
| <i>profile-name</i> | AP profile name. |
| detailed | Shows the detailed parameters of the AP join profile. |
| hyperlocation | Shows Hyperlocation information for the AP profile. |
| ble-beacon | Show the list of configured BLE beacons for the AP profile. |
| detail | Shows detailed status of Hyperlocation for the AP profile. |
| summary | Shows overall status of Hyperlocation for the AP profile |
| <i>chassis-number</i> | Chassis number as either 1 or 2. |
| active R0 | Active instance in Route-processor slot 0. |
| standby R0 | Standby instance in Route-processor slot 0. |

Command Default None

Command Modes Privileged EXEC

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

Examples

The following example shows how to see the overall status of Hyperlocation for an AP profile:

```
Device# show ap profile my-ap-profile detailed
```

show ap rf-profile name

To display the selected ap RF-Profile details, use the **show ap rf-profile name** command.

show ap rf-profile name *profile-name* **detail**

| | | |
|---------------------------|----------------------------|-------------------------------------|
| Syntax Description | <i>profile-name</i> | Name of the RF-Profile. |
| | detail | Show detail of selected RF Profile. |
| Command Default | None | |
| Command Modes | Privileged EXEC | |
| Command History | Release | Modification |
| | Cisco IOS XE Denali 16.3.1 | This command was introduced. |
| Usage Guidelines | None | |

This example shows how to display the details of the selected RF-Profile.

```

Device#show ap rf-profile name doctest detail
Description :
AP Group Names :
RF Profile Name : doctest
Band : 2.4 GHz
802.11n client only : Disabled
Transmit Power Threshold v1: -70 dBm
Min Transmit Power: -10 dBm
Max Transmit Power: 30 dBm
Operational Rates
 802.11b 1M Rate : Mandatory
 802.11b 2M Rate : Mandatory
 802.11b 5.5M Rate : Mandatory
 802.11b 11M Rate : Mandatory
 802.11b 6M Rate : Mandatory
 802.11b 9M Rate : Supported
 802.11b 12M Rate : Supported
 802.11b 18M Rate : Supported
 802.11b 24M Rate : Supported
 802.11b 36M Rate : Supported
 802.11b 48M Rate : Supported
 802.11b 54M Rate : Supported
Max Clients : 200
Wlan name                               Max Clients
-----
Trap Threshold
  Clients: 12 clients
  Interference: 10%
  Noise: -70 dBm
  Utilization: 80%
Multicast Data Rate: auto
Rx SOP Threshold : auto
Band Select

```

show ap rf-profile name

```
Probe Response: Disabled
Cycle Count: 2 cycles
Cycle Threshold: 200 milliseconds
Expire Suppression: 20 seconds
Expire Dual Band: 60 seconds
Client RSSI: -80 dBm
Client Mid RSSI: -80 dBm
Load Balancing
Window: 5 clients
Denial: 3 count
Coverage Data
Data: -80 dBm
Voice: -80 dBm
Minimum Client Level: 3 clients
Exception Level: 25%
DCA Channel List : 1,5,9,13
DCA Foreign AP Contribution : Enabled
802.11n MCS Rates
MCS 0 : Enabled
MCS 1 : Enabled
MCS 2 : Enabled
MCS 3 : Enabled
MCS 4 : Enabled
MCS 5 : Enabled
MCS 6 : Enabled
MCS 7 : Enabled
MCS 8 : Enabled
MCS 9 : Enabled
MCS 10 : Enabled
MCS 11 : Enabled
MCS 12 : Enabled
MCS 13 : Enabled
MCS 14 : Enabled
MCS 15 : Enabled
MCS 16 : Enabled
MCS 17 : Enabled
MCS 18 : Enabled
MCS 19 : Enabled
MCS 20 : Enabled
MCS 21 : Enabled
MCS 22 : Enabled
MCS 23 : Enabled
MCS 24 : Enabled
MCS 25 : Enabled
MCS 26 : Enabled
MCS 27 : Enabled
MCS 28 : Enabled
MCS 29 : Enabled
MCS 30 : Enabled
MCS 31 : Enabled
State : Down
```

show ap rf-profile summary

To display the ap RF-Profile summary, use the **show ap rf-profile summary** command.

show ap rf-profile summary

| | | |
|---------------------------|----------------------------|------------------------------|
| Syntax Description | summary | Show summary of RF Profiles |
| Command Default | None | |
| Command Modes | Privileged EXEC | |
| Command History | Release | Modification |
| | Cisco IOS XE Denali 16.3.1 | This command was introduced. |
| Usage Guidelines | None | |

This example shows how to display the ap RF-Profile summary .

```
Device#show ap rf-profile summary
```

```
Number of RF Profiles : 1
```

| RF Profile Name | Band | Description | Applied | State |
|-----------------|---------|-------------|---------|-------|
| doctest | 2.4 GHz | | No | Down |

show ap sensor status

To display the details of the AP sensors and their status, use the **show ap sensor status** command.

show ap sensor status

| | |
|---------------------------|--------------------------------|
| Syntax Description | This command has no arguments. |
|---------------------------|--------------------------------|

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

| | |
|----------------------|---------------------|
| Command Modes | Privileged EXEC (#) |
|----------------------|---------------------|

| Command History | Release | Modification |
|------------------------|-------------------------------|------------------------------|
| | Cisco IOS XE Cupertino 17.8.1 | This command was introduced. |

Example

The following example displays the details of the AP sensors and their status:

```
Device# show ap sensor status
```

show ap summary

To display the status summary of all Cisco lightweight access points attached to the device, use the **show ap summary** command.

show ap summary

| | | |
|---------------------------|--|------------------------------|
| Syntax Description | This command has no keywords and arguments. | |
| Command Default | None | |
| Command Modes | Any command mode | |
| Command History | Release | Modification |
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |
| Usage Guidelines | Use this command to display a list that contains each lightweight access point name, number of slots, manufacturer, MAC address, location, and the device port number. | |

This example shows how to display a summary of all connected access points:

```
Controller# show ap summary
```

```
Number of APs: 1
```

```
Global AP User Name: Cisco
```

```
Global AP Dot1x User Name: Not configured
```

| AP Name | AP Model | Ethernet MAC | Radio MAC | State |
|---------|----------|----------------|----------------|------------|
| 3602a | 3502I | 003a.99eb.3fa8 | d0c2.8267.8b00 | Registered |

show ap summary load-info

To view the AP per radio channel utilization and the total number of clients and slots per AP, use the **show ap summary load-info** command.

show ap summary load-info

| | |
|---------------------------|--|
| Syntax Description | This command has no arguments or keywords. |
|---------------------------|--|

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

| | |
|----------------------|---------------------|
| Command Modes | Privileged EXEC (#) |
|----------------------|---------------------|

| | | |
|------------------------|-------------------------------|------------------------------|
| Command History | Release | Modification |
| | Cisco IOS XE Amsterdam 17.3.1 | This command was introduced. |

Example

This example shows how to view the AP per radio channel utilization and the total number of clients and slots per AP:

```
Device# show ap summary load-info
```

| WTP-Mac | AP-Name | Tot-Slots | Tot-Clients | Slot0 | Slot1 |
|----------------|------------------|-----------|-------------|----------------|---------|
| | Slot2 | | | Utilisation(%) | Clients |
| 04eb.409e.a5c0 | AP04EB.409E.07EC | 3 | 0 | 0 | 99 |
| 1880.90fd.6b40 | paxxxxi-AP | 2 | 0 | 0 | 0 |
| | NA | | | | |

show ap summary sort name

To view the access point (AP) summary sorted by name, use the **show ap summary sort name** command.

show ap summary sort name

| | |
|---------------------------|--|
| Syntax Description | This command has no keywords or arguments. |
|---------------------------|--|

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

| | |
|----------------------|--------------------|
| Command Modes | Privileged EXEC(#) |
|----------------------|--------------------|

| | | |
|------------------------|-------------------------------|------------------------------|
| Command History | Release | Modification |
| | Cisco IOS XE Cupertino 17.7.1 | This command was introduced. |

Examples

This example shows how to view the AP summary sorted by name:

```
Device# show ap summary sort name
Number of APs: 05
AP Name          Slots  AP Model          Ethernet MAC      Radio MAC          Location
Country  IP Address  State
-----
ABC                2    AIR-AP1832I-D-K9  2c0b.e9b6.3618   2c0b.e9b7.3ec0   Real-AP-Testbed
IN      1.2.22.222  Registered
AP-Farm-1832I-4  2    AIR-AP1832I-D-K9  2c0b.e9b6.3e58   2c0b.e9b7.5fc0   Real-AP-Testbed
IN      1.2.22.22  Registered
AP-Farm-1832I-5  2    AIR-AP1832I-D-K9  2c0b.e9b6.3f60   2c0b.e9b7.63e0   Real-AP-Testbed
IN      1.2.22.22  Registered
AP-Farm-1832I-6  2    AIR-AP1832I-D-K9  2c0b.e9b6.3fe8   2c0b.e9b7.6600   Real-AP-Testbed
IN      1.2.22.22  Registered
AP-Farm-1832I-7  2    AIR-AP1832I-D-K9  2c0b.e9b6.4010   2c0b.e9b7.66a0   Real-AP-Testbed
IN      1.2.22.222
```

show ap summary sort ascending client-count

To view the AP summary sorted ascendingly based on the client count, use the **show ap summary sort ascending client-count** command.

show ap summary sort ascending client-count

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|--------------------------------|------------------------------|
| | Cisco IOS XE Amsterdam 17.1.1s | This command was introduced. |

This example shows how to view the AP summary sorted ascendingly based on the client count:

Device# **show ap summary sort ascending client-count**

| AP-name | Through-Put | Admin-State | AP-mac | Client count | Data Usage |
|------------|-------------|-------------|----------------|--------------|------------|
| L2_3802I_1 | | | 7872.5d27.b8c0 | 1 | 622358 |
| 11 | | Enabled | | | |
| L2_1815w_1 | | | 707d.b99e.c2e0 | 2 | 5871836 |
| 1422 | | Enabled | | | |

show ap summary sort ascending data-usage

To view the AP summary sorted ascendingly based on the data usage, use the **show ap summary sort ascending data-usage** command.

show ap summary sort ascending data-usage

| | | |
|---------------------------|--|------------------------------|
| Syntax Description | This command has no keywords or arguments. | |
| Command Default | None | |
| Command Modes | Privileged EXEC | |
| Command History | Release | Modification |
| | Cisco IOS XE Amsterdam 17.1.1s | This command was introduced. |

This example shows how to view the AP summary sorted ascendingly based on the data usage:

Device# **show ap summary sort ascending data-usage**

| AP-name | Through-Put | Admin-State | AP-mac | Client count | Data Usage |
|------------|-------------|-------------|----------------|--------------|------------|
| L2_3802I_1 | 4 | Enabled | 7872.5d27.b8c0 | 1 | 622600 |
| L2_1815w_1 | 281 | Enabled | 707d.b99e.c2e0 | 2 | 6102216 |

show ap summary sort ascending throughput

To view the AP summary sorted ascendingly based on the throughput, use the **show ap summary sort ascending throughput** command.

show ap summary sort ascending throughput

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|--------------------------------|------------------------------|
| | Cisco IOS XE Amsterdam 17.1.1s | This command was introduced. |

This example shows how to view the AP summary sorted ascendingly based on the throughput:

Device# **show ap summary sort ascending throughput**

| AP-name | Through-Put | Admin-State | AP-mac | Client count | Data Usage |
|------------|-------------|-------------|----------------|--------------|------------|
| L2_3802I_1 | 6 | Enabled | 7872.5d27.b8c0 | 1 | 6749385 |
| L2_1815w_1 | 35 | Enabled | 707d.b99e.c2e0 | 2 | 94748042 |

show ap summary sort descending client-count

To view the AP summary sorted descendingly based on the client count, use the **show ap summary sort descending client-count** command.

show ap summary sort descending client-count

| | | |
|---------------------------|--|------------------------------|
| Syntax Description | This command has no keywords or arguments. | |
| Command Default | None | |
| Command Modes | Privileged EXEC | |
| Command History | Release | Modification |
| | Cisco IOS XE Amsterdam 17.1.1s | This command was introduced. |

This example shows how to view the AP summary sorted descendingly based on the client count:

Device# **show ap summary sort descending client-count**

| AP-name | Through-Put | Admin-State | AP-mac | Client count | Data Usage |
|------------|-------------|-------------|----------------|--------------|------------|
| L2_1815w_1 | | | 707d.b99e.c2e0 | 2 | 94753989 |
| 46 | | Enabled | | | |
| L2_3802I_1 | | | 7872.5d27.b8c0 | 1 | 6750526 |
| 6 | | Enabled | | | |

show ap summary sort descending data-usage

To view the AP summary sorted descendingly based on the data usage, use the **show ap summary sort descending data-usage** command.

show ap summary sort descending data-usage

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|--------------------------------|------------------------------|
| | Cisco IOS XE Amsterdam 17.1.1s | This command was introduced. |

This example shows how to view the AP summary sorted descendingly based on the data usage:

Device# **show ap summary sort descending data-usage**

| AP-name | Through-Put | Admin-State | AP-mac | Client count | Data Usage |
|------------|-------------|-------------|----------------|--------------|------------|
| L2_1815w_1 | 47 | Enabled | 707d.b99e.c2e0 | 2 | 94756618 |
| L2_3802I_1 | 6 | Enabled | 7872.5d27.b8c0 | 0 | 6750526 |

show ap summary sort descending throughput

To view the AP summary sorted descendingly based on the throughput, use the **show ap summary sort descending throughput** command.

show ap summary sort descending throughput

| | | |
|---------------------------|--|------------------------------|
| Syntax Description | This command has no keywords or arguments. | |
| Command Default | None | |
| Command Modes | Privileged EXEC | |
| Command History | Release | Modification |
| | Cisco IOS XE Amsterdam 17.1.1s | This command was introduced. |

This example shows how to view the AP summary sorted descendingly based on the throughput:

Device# **show ap summary sort descending throughput**

| AP-name | Through-Put | Admin-State | AP-mac | Client count | Data Usage |
|------------|-------------|-------------|----------------|--------------|------------|
| L2_1815w_1 | 23 | Enabled | 707d.b99e.c2e0 | 2 | 94758750 |
| L2_3802I_1 | 6 | Enabled | 7872.5d27.b8c0 | 0 | 6750526 |

show ap support-bundle summary

To display the summary of the AP support-bundle, use the **show ap support-bundle summary** command.

show ap support-bundle summary

| | | |
|---------------------------|--|------------------------------|
| Syntax Description | This command has no keywords or arguments. | |
| Command Default | None | |
| Command Modes | Privilege EXEC (#) | |
| Command History | Release | Modification |
| | Cisco IOS XE Amsterdam 17.3.1 | This command was introduced. |

Example

This examples displays the summary of the AP support-bundle:

```
Device# show ap support-bundle summary
```


show ap tag sources

To see AP tag sources with priorities, use the **show ap tag sources** command.

```
show ap tag sources [chassis {chassis-number | active | standby} R0]
```

Syntax Description

chassis-number Chassis number as either 1 or 2.

active R0 Active instance of the AP filters in Route-processor slot 0.

standby R0 Standby instance of the AP filters in Route-processor slot 0.

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Examples

The following example shows how to see the AP tag sources with priorities for the active instance:

```
Device# show ap tag sources chassis active R0
```

show ap tag summary

To view brief summary of tag names, use the **show ap tag summary** command.

show ap tag summary

| | |
|---------------------------|--|
| 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. |

Example

The following example shows how to view brief summary of tag names:

```
Device# show ap tag summary
```

show ap triradio summary

To view the tri-radio summary, and to verify if the slots are enabled and up, use the **show ap triradio summary** command.

show ap triradio summary

| Syntax Description | This command has no keywords or arguments. | | | | |
|-------------------------------|---|---------|--------------|-------------------------------|------------------------------|
| Command Default | None | | | | |
| Command Modes | Privilege EXEC (#) | | | | |
| Command History | <table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>Cisco IOS XE Amsterdam 17.2.1</td><td>This command was introduced.</td></tr></tbody></table> | Release | Modification | Cisco IOS XE Amsterdam 17.2.1 | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE Amsterdam 17.2.1 | This command was introduced. | | | | |

Example

This example displays the tri-radio summary, and to verify if the slots are enabled:

```
Device# show ap triradio summary
```

show ap timezone

To check the AP timezone information, use the **show ap timezone** command.

show ap timezone

Syntax Description This command has no keywords and arguments.

Command Default None

Command Modes Privileged EXEC (#)

| Command History | Release | Modification |
|-----------------|-------------------------------|------------------------------|
| | Cisco IOS XE Bengaluru 17.6.1 | This command was introduced. |

Examples

The following example shows how to check the AP timezone information:

```
Device# show ap timezone
```

```
AP Name      Status      Offsets(h/m)
-----
AP1          Disabled    0:0
AP2          Enabled     1:0
```

show ap upgrade

To see AP upgrade information, use the **show ap upgrade** command.

```
show ap upgrade [{name ap-upgrade-report-name | summary | chassis {chassis-number | active | standby}]
```

Syntax Description

| | |
|---|---|
| name <i>ap-upgrade-report-name</i> | Enter the name of the AP upgrade report. |
| summary | Shows a summary of AP upgrade information. |
| <i>chassis-number</i> | Enter the chassis number as either 1 or 2. |
| active R0 | Active instance in Route-processor slot 0. |
| standby R0 | Standby instance in Route-processor slot 0. |

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Examples

The following example shows how to see a summary of the AP upgrade information:

```
Device# show ap upgrade summary
```

show ap upgrade method

To verify the status of the configuration of the image download over HTTPS method, use the **show ap upgrade method** command.

show ap upgrade method

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC (#)

| Command History | Release | Modification |
|-----------------|-----------------------------|------------------------------|
| | Cisco IOS XE Dublin 17.11.1 | This command was introduced. |

Examples

The following example shows how to verify the status of HTTPS image download configuration:

```
Device# show ap upgrade method

AP upgrade method https : Enabled
```

show arp

To view the ARP table, use the **show arp** command.

show arp

Syntax Description

arp Shows ARP table

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

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

The following example shows a sample output of the command:

```
Device# show arp
Address Age (min)      Hardware Addr
 9.11.8.1             0 84:80:2D:A0:D2:E6
9.11.32.111           0 3C:77:E6:02:33:3F
```

show arp summary

To see the ARP table summary, use the **show arp summary** command.

```
show arp summary
```

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Examples

The following example shows how to see the ARP table summary:

```
Device# show arp summary
```


show ap tunnel eogre events

To display the Ethernet over GRE (EoGRE) tunnel events, use the **show ap tunnel eogre events** command.

show ap tunnel eogre events

| | | |
|---------------------------|--|------------------------------|
| Syntax Description | This command has no keywords or arguments. | |
| Command Default | None | |
| Command Modes | Privileged EXEC (#) | |
| Command History | Release | Modification |
| | Cisco IOS XE Gibraltar 16.11.1 | This command was introduced. |

Example

This example shows how to display the EoGRE tunnel events:

```
Device# show ap tunnel eogre events
```

```
AP 80e8.6fd4.9520  Event history
Timestamp          #Times  Event                               RC Context
-----
02/18/2019 23:50:26.341 6      IAPP_STATS                          0 GW Tunnel2 uptime:0s
02/18/2019 23:49:40.222 2      CLIENT_JOIN                          0 74da.3828.88b0, (eogre_domain/2121)
02/18/2019 23:48:43.549 1      CLIENT_LEAVE                         0 74da.3828.88b0, (eogre_domain/2121)
02/18/2019 23:47:33.127 1      DOMAIN_STATUS                       0 eogre_domain Active GW: Tunnel1
02/18/2019 23:47:33.124 4      AP_TUNNEL_STATUS                    0 Tunnel2 Dn
02/18/2019 23:47:33.124 1      MSG_CLIENT_DEL                      0 GW Tunnel2 (IP: 9.51.1.12)
02/18/2019 23:47:33.124 2      TUNNEL_ADD                          0 GW Tunnel2
02/18/2019 23:47:33.120 3      MSG_CLIENT_DEL_PD                   0 GW Tunnel1 (IP: 9.51.1.11)
02/18/2019 23:47:31.763 2      AP_DOMAIN_PUSH                      0 Delete:eogre_domain_set, 0 GWs
02/18/2019 23:47:31.753 4      AP_VAP_PUSH                          0 profile:'eogre_tunnel',
wlan:pyats_eogre
```

show ap tunnel eogre domain detailed

To display the detailed information of the Ethernet over GRE (EoGRE) tunnel domain status on an AP, use the **show ap tunnel eogre domain detailed** command.

show ap tunnel eogre domain detailed *domain-name*

| Syntax Description | <i>domain-name</i> EoGRE domain name. | | | | |
|--------------------------------|--|---------|--------------|--------------------------------|------------------------------|
| Command Default | None | | | | |
| Command Modes | Privileged EXEC (#) | | | | |
| Command History | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.11.1</td> <td>This command was introduced.</td> </tr> </tbody> </table> | Release | Modification | Cisco IOS XE Gibraltar 16.11.1 | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE Gibraltar 16.11.1 | This command was introduced. | | | | |

Example

This example shows how to display the detailed information of the EoGRE tunnel domain status:

```
Device# show ap tunnel eogre domain detailed Tunnell
```

```
Gateway : Tunnell
Mode    : IPv4
IP      : 9.51.1.11
State   : Up
MTU     : 1476
Up Time: 14 hours 25 minutes 2 seconds
AP MAC  : 80e8.6fd4.9520

Clients
  Total Number of Wireless Clients      : 1
Traffic
  Total Number of Received Packets     : 6
  Total Number of Received Bytes       : 2643
  Total Number of Transmitted Packets  : 94
  Total Number of Transmitted Bytes    : 20629
  Total Number of Lost Keepalive       : 3
```

show ap name tunnel eogre domain summary

To display the summary information of the Ethernet over GRE (EoGRE) tunnel domain on an AP, use the **show ap nametunnel eogre domain summary** command.

show ap name *ap-name* **tunnel eogre domain summary**

| Syntax Description | <i>ap-name</i> AP name. | | | | |
|--------------------------------|--|---------|--------------|--------------------------------|------------------------------|
| Command Default | None | | | | |
| Command Modes | Privileged EXEC (#) | | | | |
| Command History | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.11.1</td> <td>This command was introduced.</td> </tr> </tbody> </table> | Release | Modification | Cisco IOS XE Gibraltar 16.11.1 | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE Gibraltar 16.11.1 | This command was introduced. | | | | |

Example

This example shows how to display the summary information of the EoGRE tunnel domain on an AP:

```
Device# show ap name ap1 tunnel eogre domain summary
```

```
AP MAC           Domain           Active Gateway
-----
80e8.6fd4.9520  eogre_domain    Tunnell
```

show ap tunnel eogre gateway detailed

To display the detailed information of the Ethernet over GRE (EoGRE) tunnel gateway status on an AP, use the **show ap name tunnel eogre gateway detailed** command.

show ap name *ap-name* **tunnel eogre gateway detailed** *gateway-name*

| | | |
|---------------------------|--------------------------------|------------------------------|
| Syntax Description | <i>ap-name</i> | AP name. |
| | <i>gateway-name</i> | EoGRE domain name. |
| Command Default | None | |
| Command Modes | Privileged EXEC (#) | |
| Command History | Release | Modification |
| | Cisco IOS XE Gibraltar 16.11.1 | This command was introduced. |

Example

This example shows how to display the detailed information of the EoGRE tunnel gateway status on an AP:

```
Device# show ap name ap1 tunnel eogre gateway detailed Tunnell
```

```
Gateway : Tunnell
Mode    : IPv4
IP      : 9.51.1.11
State   : Up
MTU     : 1476
Up Time: 14 hours 25 minutes 2 seconds
AP MAC  : 80e8.6fd4.9520

Clients
  Total Number of Wireless Clients      : 1
Traffic
  Total Number of Received Packets     : 6
  Total Number of Received Bytes       : 2643
  Total Number of Transmitted Packets   : 94
  Total Number of Transmitted Bytes     : 20629
  Total Number of Lost Keepalive       : 3
```

show ap tunnel eogre gateway summary

To display the summary information of the Ethernet over GRE (EoGRE) tunnel gateway, use the **show ap tunnel eogre gateway summary** command.

show ap tunnel eogre gateway summary

| Syntax Description | This command has no keywords or arguments. | | | | |
|--------------------------------|--|---------|--------------|--------------------------------|------------------------------|
| Command Default | None | | | | |
| Command Modes | Privileged EXEC (#) | | | | |
| Command History | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.11.1</td> <td>This command was introduced.</td> </tr> </tbody> </table> | Release | Modification | Cisco IOS XE Gibraltar 16.11.1 | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE Gibraltar 16.11.1 | This command was introduced. | | | | |

Example

This example shows how to display the summary information of the EoGRE tunnel gateway:

```
Device# show ap tunnel eogre gateway summary
```

| AP MAC | Gateway | Type | IP | State | Clients |
|----------------|---------|------|-----------|-------|---------|
| 80e8.6fd4.9520 | Tunnel1 | IPv4 | 9.51.1.11 | Up | 1 |
| 80e8.6fd4.9520 | Tunnel2 | IPv4 | 9.51.1.12 | Down | 0 |

show ap upgrade site

To view the upgrade site-related information, use the **show ap upgrade site** command.

show ap upgrade site [**summary**]

| Syntax Description | summary (Optional) Displays a summary of access point (AP) upgrade on individual sites. | | | | |
|-------------------------------|---|---------|--------------|-------------------------------|------------------------------|
| Command Default | None | | | | |
| Command Modes | Privileged EXEC (#) | | | | |
| Command History | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Cupertino 17.9.1</td> <td>This command was introduced.</td> </tr> </tbody> </table> | Release | Modification | Cisco IOS XE Cupertino 17.9.1 | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE Cupertino 17.9.1 | This command was introduced. | | | | |

Examples

The following example shows how to view the upgrade site-related information:

```
Device# show ap upgrade site

Site-filtered AP upgrade report data
=====
Source controller: Controller1
Destination controller: Controller2
Site-filters present: Yes

AP image upgrade site summary
-----
Operation: N+1 move

Site Tag                               Status
-----
site1                                   In Progress

AP upgrade reports linked to these site-filters
-----

Start time           Operation type           Report name
-----
01/30/2022 10:34:36 IST AP image upgrade/move CLI AP_upgrade_to_Controller2_3002022103435
```

show avc client

To display information about top number of applications, use the **show avc client** command in privileged EXEC mode.

```
show avc client client-mac top n application [aggregate | upstream | downstream]
```

Syntax Description

client *client-mac* Specifies the client MAC address.

top n application Specifies the number of top "N" applications for the given client.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

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

The following is sample output from the **show avc client** command:

```
Device# sh avc client 0040.96ae.65ec top 10 application aggregate
```

Cumulative Stats:

| No. | AppName | Packet-Count | Byte-Count | AvgPkt-Size | usage% |
|-----|---------|--------------|------------|-------------|--------|
| 1 | skinny | 7343 | 449860 | 61 | 94 |
| 2 | unknown | 99 | 13631 | 137 | 3 |
| 3 | dhcp | 18 | 8752 | 486 | 2 |
| 4 | http | 18 | 3264 | 181 | 1 |
| 5 | tftp | 9 | 534 | 59 | 0 |
| 6 | dns | 2 | 224 | 112 | 0 |

Last Interval (90 seconds) Stats:

| No. | AppName | Packet-Count | Byte-Count | AvgPkt-Size | usage% |
|-----|---------|--------------|------------|-------------|--------|
| 1 | skinny | 9 | 540 | 60 | 100 |

show avc wlan

To display information about top applications and users using the applications, use the **show avc wlan** command in privileged EXEC mode.

show avc wlan ssid top n application [aggregate | upstream | downstream]

| Syntax Description | Parameter | Description |
|--------------------|--------------------------|---|
| | wlan ssid | Specifies the Service Set Identifier (SSID) for WLAN. |
| | top n application | Specifies the number of top "N" applications. |

Command Default No default behavior or values.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

The following is sample output from the **show avc wlan** command:

```
Device# show avc wlan Lobby_WLAN top 10 application aggregate
```

Cumulative Stats:

| No. | AppName | Packet-Count | Byte-Count | AvgPkt-Size | usage% |
|-----|------------------|--------------|------------|-------------|--------|
| 1 | ssl | 10598677 | 1979525706 | 997 | 42 |
| 2 | vnc | 5550900 | 3764612847 | 678 | 14 |
| 3 | http | 3043131 | 2691327197 | 884 | 10 |
| 4 | unknown | 1856297 | 1140264956 | 614 | 4 |
| 5 | video-over-http | 1625019 | 2063335150 | 1269 | 8 |
| 6 | binary-over-http | 1329115 | 1744190344 | 1312 | 6 |
| 7 | webex-meeting | 1146872 | 540713787 | 471 | 2 |
| 8 | rtp | 923900 | 635650544 | 688 | 2 |
| 9 | unknown | 752341 | 911000213 | 1210 | 3 |
| 10 | youtube | 631085 | 706636186 | 1119 | 3 |

Last Interval(90 seconds) Stats:

| No. | AppName | Packet-Count | Byte-Count | AvgPkt-Size | usage% |
|-----|-----------------|--------------|------------|-------------|--------|
| 1 | vnc | 687093 | 602731844 | 877 | 68 |
| 2 | video-over-http | 213272 | 279831588 | 1312 | 31 |
| 3 | ssl | 6515 | 5029365 | 771 | 1 |
| 4 | webex-meeting | 3649 | 1722663 | 472 | 0 |
| 5 | http | 2634 | 1334355 | 506 | 0 |
| 6 | unknown | 1436 | 99412 | 69 | 0 |
| 7 | google-services | 722 | 378121 | 523 | 0 |
| 8 | linkedin | 655 | 393263 | 600 | 0 |
| 9 | exchange | 432 | 167390 | 387 | 0 |
| 10 | gtalk-chat | 330 | 17330 | 52 | 0 |

show awips wlc-alarm

To view the contents of the AWIPS WLC Alarm table, use the **show awips wlc-alarm** command.

show awips wlc-alarm

| | |
|---------------------------|--|
| Syntax Description | This command has no keywords or arguments. |
|---------------------------|--|

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

| | |
|----------------------|---------------------|
| Command Modes | Privileged EXEC (#) |
|----------------------|---------------------|

| | | |
|------------------------|-------------------------------|-----------------------------|
| Command History | Release | Modification |
| | Cisco IOS XE Amsterdam 17.3.1 | This command was introduced |

Examples

The following example shows how to view the contents of the AWIPS WLC Alarm table:

```
Device# show awips wlc-alarm
```

| Time | BSSID | Client MAC | Alarm description |
|---------------------|----------------|----------------|-------------------------|
| 04/02/2020 16:03:18 | e4aa.5d53.b921 | 74da.3864.2a94 | WPA2 Key Reinstal KRACK |
| 04/02/2020 16:03:19 | e4aa.5d53.b921 | 74da.3864.2a94 | WPA2 Key Reinstal KRACK |
| 04/02/2020 16:03:20 | e4aa.5d53.b921 | 74da.3864.2a94 | WPA2 Key Reinstal KRACK |
| 04/02/2020 16:03:21 | e4aa.5d53.b921 | 74da.3864.2a94 | WPA2 Key Reinstal KRACK |

show awips syslog throttle

To verify the syslog configuration for Cisco Advanced Wireless Intrusion Prevention System (aWIPS), use the **show awips syslog throttle** command.

show awips syslog throttle

| | | |
|---------------------------|--|------------------------------|
| Syntax Description | This command has no keywords or arguments. | |
| Command Default | None | |
| Command Modes | Privileged EXEC | |
| Command History | Release | Modification |
| | Cisco IOS XE Bengaluru 17.6.1 | This command was introduced. |

The following example shows how to verify the syslog configuration for aWIPS:

```
Device# show awips syslog throttle
Syslog Throttle Interval (seconds)
-----
60
```

show capwap client rcb

To view the CAPWAP status and modes, use the **show capwap client rcb** command on the access point.

show capwap client rcb

| | | |
|---------------------------|---|------------------------------|
| Syntax Description | This command has no keywords and arguments. | |
| Command Default | None | |
| Command Modes | Privileged EXEC (#) | |
| Command History | Release | Modification |
| | Cisco IOS XE Amsterdam 17.3.1 | This command was introduced. |

Example

This example shows how to view the CAPWAP status and modes on the access point:

```
AP# show capwap client rcb

OperationState           : UP
Name                     : AP4001.7A39.2D5A
MwarHwVer                : 0.0.0.0
Location                 : default location
ApMode                   : Remote Bridge
ApSubMode                : Not Configured
CAPWAP Path MTU         : 1485
Software Initiated Reload Reason : Reload command
CAPWAP Sliding Window
Active Window Size       : 10
Last Request Send To Application : 184
Expected Seq Num         : 185
Received Seq Num         : 184
Request Packet Count     : 42424
Out Of Range Packets Count : 0
Window Moved Packets Count : 0
In Range Packets Count   : 960
Expected Packets Count   : 41464
```

show chassis

To see the chassis information, use the **show chassis** command.

```
show chassis [{1 | 2} | detail | mode | neighbors | ha-status {active | local | standby}]
```

Syntax Description

| | |
|------------------|---|
| {1 2} | Chassis number as 1 or 2 to see the information about the relevant chassis. |
| detail | Shows detailed information about the chassis. |
| mode | Shows information about the chassis mode. |
| neighbors | Shows information about the chassis neighbors. |
| ha-status | Option to see information about the High Availability (HA) status. |
| active | Shows HA status on the chassis that is in active state. |
| local | Shows HA status on the local chassis. |
| standby | Shows HA status on the chassis that is in standby state. |

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Examples

The following example shows how to see the HA status on the active chassis:

```
Device# show chassis ha-status active
```

show chassis rmi

To verify the chassis Redundancy Management Interface (RMI) configuration for an active controller, use the **show chassis rmi** command.

show chassis rmi

| | | |
|---------------------------|--|------------------------------|
| Syntax Description | This command has no keywords or arguments. | |
| Command Default | None | |
| Command Modes | Privileged EXEC | |
| Command History | Release | Modification |
| | Cisco IOS XE Amsterdam 17.1.1 | This command was introduced. |

This example shows how to verify the chassis Redundancy Management Interface (RMI) configuration for an active controller:

```
Device# show chassis rmi
Chassis/Stack Mac Address : 000c.2964.1eb6 - Local Mac Address
Mac persistency wait time: Indefinite
H/W Current
Chassis# Role Mac Address Priority Version State IP RMI-IP
-----
*1 Active 000c.2964.1eb6 1 V02 Ready 169.254.90.147 9.10.90.147
2 Standby 000c.2975.3aa6 1 V02 Ready 169.254.90.149 9.10.90.149
```

show checkpoint

To display information about the Checkpoint Facility (CF) subsystem, use the **show checkpoint** command.

show checkpoint { **clients** *client-ID* <0-381> | **entities** *entity-ID* <1-7> | **statistics** **buffer-usage** }

Syntax Description

| | |
|---------------------|--|
| clients | Displays detailed information about checkpoint clients. |
| entities | Displays detailed information about checkpoint entities. |
| statistics | Displays detailed information about checkpoint statistics. |
| buffer-usage | Displays the checkpoint statistics of clients using large number of buffers. |

Command Default

None

Command Modes

Privileged EXEC

Command History

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

This example shows how to display all the CF clients.

```

Client residing in process : 8135
-----
Checkpoint client: WCM_MOBILITY
  Client ID                : 24105
  Total DB inserts         : 0
  Total DB updates         : 0
  Total DB deletes        : 0
  Total DB reads           : 0
  Number of tables         : 6
  Client residing in process : 8135
-----
Checkpoint client: WCM_DOT1X
  Client ID                : 24106
  Total DB inserts         : 2
  Total DB updates         : 1312
  Total DB deletes        : 2
  Total DB reads           : 0
  Number of tables         : 1
  Client residing in process : 8135
-----
Checkpoint client: WCM_APFROGUE
  Client ID                : 24107
  Total DB inserts         : 0
  Total DB updates         : 0
  Total DB deletes        : 0
  Total DB reads           : 0
  Number of tables         : 1
  Client residing in process : 8135
-----
Checkpoint client: WCM_CIDS
  Client ID                : 24110
  Total DB inserts         : 0

```

```
Total DB updates      : 0
Total DB deletes      : 0
Total DB reads        : 0
Number of tables      : 0
Client residing in process : 8135
```

```
-----
Checkpoint client: WCM_NETFLOW
Client ID              : 24111
Total DB inserts       : 7
Total DB updates       : 0
Total DB deletes       : 0
Total DB reads         : 0
Number of tables       : 1
Client residing in process : 8135
```

```
-----
Checkpoint client: WCM_MCAST
Client ID              : 24112
Total DB inserts       : 0
Total DB updates       : 0
Total DB deletes       : 0
Total DB reads         : 0
Number of tables       : 1
Client residing in process : 8135
```

```
-----
Checkpoint client: wcm_comet
Client ID              : 24150
Total DB inserts       : 0
Total DB updates       : 0
Total DB deletes       : 0
Total DB reads         : 0
Number of tables       : 0
Client residing in process : 8135
```

All iosd checkpoint clients

```
-----
Client Name           Client      Entity      Bundle
                    ID          ID          Mode
-----
```

| Client Name | Client ID | Entity ID | Bundle Mode |
|-------------------|-----------|-----------|-------------|
| Network RF Client | 3 | -- | Off |

```
-----
Total API Messages Sent:          0
Total Transport Messages Sent:    0
Length of Sent Messages:         0
Total Blocked Messages Sent:     0
Length of Sent Blocked Messages:  0
Total Non-blocked Messages Sent:  0
Length of Sent Non-blocked Messages: 0
Total Bytes Allocated:           0
Buffers Held:                    0
Buffers Held Peak:               0
Huge Buffers Requested:          0
Transport Frag Count:            0
Transport Frag Peak:             0
Transport Sends w/Flow Off:      0
Send Errs:                       0
Send Peer Errs:                 0
Rcv Xform Errs:                 0
Xmit Xform Errs:                 0
Incompatible Messages:          0
Client Unbundles to Process Memory: T
```

```
-----
Client Name           Client      Entity      Bundle
```

```

-----
                ID          ID          Mode
-----
SNMP CF Client          12          --          Off

Total API Messages Sent:                0
Total Transport Messages Sent:           0
Length of Sent Messages:                 0
Total Blocked Messages Sent:             0
Length of Sent Blocked Messages:         0
Total Non-blocked Messages Sent:         0
Length of Sent Non-blocked Messages:     0
Total Bytes Allocated:                   0
Buffers Held:                            0
Buffers Held Peak:                       0
Huge Buffers Requested:                  0
Transport Frag Count:                    0
Transport Frag Peak:                     0
Transport Sends w/Flow Off:              0
Send Errs:                               0
Send Peer Errs:                          0
Rcv Xform Errs:                          0
Xmit Xform Errs:                         0
Incompatible Messages:                   0
Client Unbundles to Process Memory:      T
-----

Client Name          Client      Entity      Bundle
                   ID          ID          Mode
-----
Online Diags HA          14          --          Off

Total API Messages Sent:                0
Total Transport Messages Sent:           0
Length of Sent Messages:                 0
Total Blocked Messages Sent:             0
Length of Sent Blocked Messages:         0
Total Non-blocked Messages Sent:         0
Length of Sent Non-blocked Messages:     0
Total Bytes Allocated:                   0
Buffers Held:                            0
Buffers Held Peak:                       0
Huge Buffers Requested:                  0
Transport Frag Count:                    0
Transport Frag Peak:                     0
Transport Sends w/Flow Off:              0
Send Errs:                               0
Send Peer Errs:                          0
Rcv Xform Errs:                          0
Xmit Xform Errs:                         0
Incompatible Messages:                   0
Client Unbundles to Process Memory:      T
-----

Client Name          Client      Entity      Bundle
                   ID          ID          Mode
-----
ARP                    22          --          Off

Total API Messages Sent:                0
Total Transport Messages Sent:           0
Length of Sent Messages:                 0
Total Blocked Messages Sent:             0
Length of Sent Blocked Messages:         0
Total Non-blocked Messages Sent:         0
Length of Sent Non-blocked Messages:     0
Total Bytes Allocated:                   0

```



```

Buffers Held: 0
Buffers Held Peak: 0
Huge Buffers Requested: 0
Transport Frag Count: 0
Transport Frag Peak: 0
Transport Sends w/Flow Off: 0
Send Errs: 0
Send Peer Errs: 0
Rcv Xform Errs: 0
Xmit Xform Errs: 0
Incompatible Messages: 0
Client Unbundles to Process Memory: T
    
```

| Client Name | Client ID | Entity ID | Bundle Mode |
|-------------|-----------|-----------|-------------|
| Tableid CF | 27 | -- | Off |

```

Total API Messages Sent: 0
Total Transport Messages Sent: 0
Length of Sent Messages: 0
Total Blocked Messages Sent: 0
Length of Sent Blocked Messages: 0
Total Non-blocked Messages Sent: 0
Length of Sent Non-blocked Messages: 0
Total Bytes Allocated: 0
Buffers Held: 0
Buffers Held Peak: 0
Huge Buffers Requested: 0
Transport Frag Count: 0
Transport Frag Peak: 0
Transport Sends w/Flow Off: 0
Send Errs: 0
Send Peer Errs: 0
Rcv Xform Errs: 0
Xmit Xform Errs: 0
Incompatible Messages: 0
Client Unbundles to Process Memory: T
    
```

| Client Name | Client ID | Entity ID | Bundle Mode |
|---------------|-----------|-----------|-------------|
| Event Manager | 33 | 0 | Off |

```

Total API Messages Sent: 0
Total Transport Messages Sent: --
Length of Sent Messages: 0
Total Blocked Messages Sent: 0
Length of Sent Blocked Messages: 0
Total Non-blocked Messages Sent: 0
Length of Sent Non-blocked Messages: 0
Total Bytes Allocated: 0
Buffers Held: 0
Buffers Held Peak: 0
Huge Buffers Requested: 0
Transport Frag Count: 0
Transport Frag Peak: 0
Transport Sends w/Flow Off: 0
Send Errs: 0
Send Peer Errs: 0
Rcv Xform Errs: 0
Xmit Xform Errs: 0
Incompatible Messages: 0
Client Unbundles to Process Memory: T
    
```

show checkpoint

```

-----
Client Name          Client      Entity      Bundle
                   ID          ID          Mode
-----
LAN-Switch Port Mana 35          0          Off

Total API Messages Sent:          0
Total Transport Messages Sent:    --
Length of Sent Messages:          0
Total Blocked Messages Sent:      0
Length of Sent Blocked Messages:  0
Total Non-blocked Messages Sent:  0
Length of Sent Non-blocked Messages: 0
Total Bytes Allocated:            0
Buffers Held:                     0
Buffers Held Peak:                0
Huge Buffers Requested:           0
Transport Frag Count:              0
Transport Frag Peak:              0
Transport Sends w/Flow Off:       0
Send Errs:                        0
Send Peer Errs:                   0
Rcv Xform Errs:                   0
Xmit Xform Errs:                   0
Incompatible Messages:            0
Client Unbundles to Process Memory: T
-----

```

```

-----
Client Name          Client      Entity      Bundle
                   ID          ID          Mode
-----
LAN-Switch PAgP/LACP 36          0          Off

Total API Messages Sent:          0
Total Transport Messages Sent:    --
Length of Sent Messages:          0
Total Blocked Messages Sent:      0
Length of Sent Blocked Messages:  0
Total Non-blocked Messages Sent:  0
Length of Sent Non-blocked Messages: 0
Total Bytes Allocated:            0
Buffers Held:                     0
Buffers Held Peak:                0
Huge Buffers Requested:           0
Transport Frag Count:              0
Transport Frag Peak:              0
Transport Sends w/Flow Off:       0
Send Errs:                        0
Send Peer Errs:                   0
Rcv Xform Errs:                   0
Xmit Xform Errs:                   0
Incompatible Messages:            0
Client Unbundles to Process Memory: T
-----

```

```

-----
Client Name          Client      Entity      Bundle
                   ID          ID          Mode
-----
LAN-Switch VLANs    39          0          Off

Total API Messages Sent:          0
Total Transport Messages Sent:    --
Length of Sent Messages:          0
Total Blocked Messages Sent:      0
Length of Sent Blocked Messages:  0
Total Non-blocked Messages Sent:  0
-----

```

```

Length of Sent Non-blocked Messages:      0
Total Bytes Allocated:                    0
Buffers Held:                             0
Buffers Held Peak:                        0
Huge Buffers Requested:                   0
Transport Frag Count:                     0
Transport Frag Peak:                       0
Transport Sends w/Flow Off:                0
Send Errs:                                0
Send Peer Errs:                           0
Rcv Xform Errs:                           0

```

This example shows how to display all the CF entities.

```

KATANA_DOC#show checkpoint entities
                        Check Point List of Entities

```

CHKPT on ACTIVE server.

```

-----
Entity ID      Entity Name
-----
          0      CHKPT_DEFAULT_ENTITY

Total API Messages Sent:      0
Total Messages Sent:         0
Total Sent Message Len:      0
Total Bytes Allocated:       0
Total Number of Members:     10

Member(s) of entity 0 are:
  Client ID      Client Name
-----
          168      DHCP Snooping
          167      IGMP Snooping
           41      Spanning-tree
           40      AUTH MGR CHKPT CLIEN
           39      LAN-Switch VLANs
           33      Event Manager
           35      LAN-Switch Port Mana
           36      LAN-Switch PAgP/LACP
          158      Inline Power Checkpoint

```

This example shows how to display the CF statistics.

```

KATANA_DOC#show checkpoint statistics
                        IOSd Check Point Status
CHKPT on ACTIVE server.

Number Of Msgs In Hold Q:      0
CHKPT MAX Message Size:       0
TP MAX Message Size:          65503
CHKPT Pending Msg Timer:      100 ms

FLOW_ON total:                 0
FLOW_OFF total:                 0
Current FLOW status is:        ON
Total API Messages Sent:       0
Total Messages Sent:           0
Total Sent Message Len:        0
Total Bytes Allocated:         0
Rcv Msg Q Peak:                0
Hold Msg Q Peak:               0

```

show checkpoint

```
Buffers Held Peak:          0
Current Buffers Held:      0
Huge Buffers Requested:    0
```

show cts environment data

To display the TrustSec environment data on the AP, use the **show cts environment data** command:

show cts environment data

| | |
|---------------------------|--|
| Syntax Description | This command has no arguments or keywords. |
|---------------------------|--|

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

| | |
|----------------------|---------------------|
| Command Modes | Privileged EXEC (#) |
|----------------------|---------------------|

| Command History | Release | Modification |
|------------------------|---------------------------|---------------------------------|
| | Cisco Amsterdam 17.1.1 | This command was introduced. |

Examples

The following example shows the TrustSec environment data on the AP:

```
Device# show cts environment
```

```
CTS Environment Data
=====
Current state = COMPLETE
Last status   = Successful
Local Device SGT:
SGT tag = 0-07:Unknown
Server List Info:
Installed list: CTSServerList1-0001, 1 server(s):
Server: 8.109.0.85, port 1812, A-ID 9818EE1ECA02B7BFE359C28B30EA7E2A
Status = ALIVE
auto-test = FALSE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs
Security Group Name Table:
0-07:Unknown
2-00:TrustSec_Devices
3-00:Network_Services
4-00:Employees
5-00:Contractors
6-00:Guests
7-00:Production_Users
8-00:Developers
9-00:Auditors
10-00:Point_of_Sale_Systems
11-02:Production_Servers
12-00:Development_Servers
13-00:Test_Servers
14-00:PCI_Servers
15-00:BYOD
16-06:BGL15
17-00:BGL12
255-00:Quarantined_Systems
Environment Data Lifetime = 86400 secs
Last update time = 11:50:49 UTC Sun Jan 9 2022
Env-data expires in 0:00:28:54 (dd:hr:mm:sec)
Env-data refreshes in 0:00:28:54 (dd:hr:mm:sec)
```

```
Cache data applied = NONE  
State Machine is running
```

show cts role-based sgt-map all

To display the bindings of IP address and SGT source names on the AP, use the **show cts role-based sgt-map all** command:

```
show cts role-based sgt-map all
```

| | |
|---------------------------|--|
| Syntax Description | This command has no arguments or keywords. |
|---------------------------|--|

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

| | |
|----------------------|---------------------|
| Command Modes | Privileged EXEC (#) |
|----------------------|---------------------|

| Command History | Release | Modification |
|------------------------|------------------------|------------------------------|
| | Cisco Amsterdam 17.1.1 | This command was introduced. |

Examples

The following example shows the bindings of IP address and SGT source names on the AP:

```
Device# show cts role-based stg-map all
```

```
Active IPv4-SGT Bindings Information
IP Address                               SGT      Source
=====
8.73.1.101                               16       LOCAL
8.73.1.102                               16       LOCAL
8.73.1.103                               16       LOCAL
8.73.1.104                               16       LOCAL
8.73.1.105                               16       LOCAL
8.73.1.106                               16       LOCAL
8.73.1.107                               16       LOCAL
8.73.1.108                               16       LOCAL
8.73.1.109                               16       LOCAL
8.73.1.110                               16       LOCAL
8.73.1.111                               16       LOCAL
8.73.1.112                               16       LOCAL
8.73.1.113                               16       LOCAL
8.73.1.114                               16       LOCAL
8.73.1.115                               16       LOCAL
8.73.1.116                               16       LOCAL
8.73.1.117                               16       LOCAL
8.73.1.118                               16       LOCAL
8.73.1.119                               16       LOCAL
8.73.1.120                               16       LOCAL
8.73.1.121                               16       LOCAL
8.73.1.122                               16       LOCAL
8.73.1.123                               16       LOCAL
8.73.1.124                               16       LOCAL
8.73.1.125                               16       LOCAL
8.73.1.126                               16       LOCAL
8.73.1.127                               16       LOCAL
8.73.1.128                               16       LOCAL
8.73.1.129                               16       LOCAL
8.73.1.130                               16       LOCAL
8.73.1.131                               16       LOCAL
```

```
show cts role-based sgt-map all
```

```
8.73.1.132          16      LOCAL
8.73.1.133          16      LOCAL
8.73.1.134          16      LOCAL
8.73.1.135          16      LOCAL
8.73.1.136          16      LOCAL
8.73.1.137          16      LOCAL
8.73.1.138          16      LOCAL
8.73.1.139          16      LOCAL
8.73.1.140          16      LOCAL
8.73.1.141          16      LOCAL
8.73.1.142          16      LOCAL
FD09:8::            16      LOCAL
FD09:8:73:0:4051:EB27:B4A2:F6DB 16      LOCAL
FD09:8:73:0:4C3C:1D75:81E0:DB94 16      LOCAL
FD09:8:73:0:5136:9045:9D11:E191 16      LOCAL
FD09:8:73:0:6903:B84E:5BDF:9D54 16      LOCAL
FD09:8:73:0:A9F8:7825:B07:75A8   16      LOCAL
FD09:8:73:0:B505:626B:51D7:6DB6 16      LOCAL
FD09:8:73:0:D0B4:3316:7CE9:8AE8  16      LOCAL
FD09:8:73:0:ECA8:F5E:CCF5:FFD7   16      LOCAL
```

```
IP-SGT Active Bindings Summary
```

```
=====
Total number of LOCAL bindings = 9
Total number of active bindings = 9
```


show cts role-based counters

To clear all role-based counters on the AP, use the **show cts role-based counters** command:

```
show cts role-based counters
```

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Privileged EXEC (#)

| Command History | Release | Modification |
|-----------------|------------------------|------------------------------|
| | Cisco Amsterdam 17.1.1 | This command was introduced. |

Examples

The following example shows the clear all role-based counters on the AP:

```
Device# show cts role-based counters
```

```

From  To   SW-Denied HW-Denied SW-Permitt HW-Permitt SW-Monitor HW-Monitor
=====
*     *     0         0         0         178837189  0         0
16    0     0         0         0         39250482   0         0
16    16    0         52835    0         0         0         0
17    16    0         0         0         0         0         0

```

show environment summary

To view a summary of all the environment-monitoring sensors, use the **show environment summary** command.

show environment summary

| | |
|---------------------------|--|
| Syntax Description | This command has no arguments or keywords. |
|---------------------------|--|

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

| | |
|----------------------|---------------------|
| Command Modes | Privileged EXEC (#) |
|----------------------|---------------------|

| Command History | Release | Modification |
|------------------------|--------------------------------|---|
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |
| | Cisco IOS XE Bengaluru 17.5.1 | This command output was modified. |

Example

The following is a sample output of the **show environment summary** command:

Example

```
Device# show environment summary
```

```
Number of Critical alarms: 0
Number of Major alarms: 0
Number of Minor alarms: 0
```

```

Slot          Sensor          Current State  Reading
Threshold(Minor,Major,Critical,Shutdown)
-----
P0            Vin              Normal         231 V AC      na
P0            Iin              Normal         2 A           na
P0            Vout             Normal         12 V DC      na
P0            Iout             Normal         30 A         na
P0            Temp1            Normal         25 Celsius (na ,na ,na ,na ) (Celsius)
P0            Temp2            Normal         31 Celsius (na ,na ,na ,na ) (Celsius)
P0            Temp3            Normal         37 Celsius (na ,na ,na ,na ) (Celsius)
R0            VDMB1: VX1      Normal         1226 mV      na
R0            VDMB1: VX2      Normal         6944 mV      na
R0            VDMB1: VX3      Normal         1226 mV      na
R0            VDMB1: VX4      Normal         1000 mV      na
R0            VDMB1: VP1      Normal         1789 mV      na
R0            VDMB1: VP2      Normal         2555 mV      na
R0            VDMB1: VP3      Normal         2556 mV      na
R0            VDMB1: VP4      Normal         1049 mV      na
R0            VDMB1: VH       Normal         11993mV     na
R0            VDMB2: VX2      Normal         4975 mV      na
R0            VDMB2: VX3      Normal         853 mV       na
R0            VDMB2: VX4      Normal         907 mV       na
```

```

R0          VDMB2: VX5      Normal      1008 mV      na
R0          VDMB2: VP1      Normal      1787 mV      na
R0          VDMB2: VP2      Normal      3323 mV      na
R0          VDMB2: VH        Normal      12003mV      na
R0          VDMB3: VX1      Normal      968 mV       na
R0          VDMB3: VX2      Normal      1002 mV      na
R0          VDMB3: VX5      Normal      5090 mV      na
R0          VDMB3: VP1      Normal      2492 mV      na
R0          VDMB3: VP2      Normal      1196 mV      na
R0          VDMB3: VP3      Normal      1512 mV      na
R0          VDMB3: VP4      Normal      1509 mV      na
R0          VDMB3: VH        Normal      11998mV      na
R0          Temp: DMB IN    Normal      26 Celsius (45 ,55 ,65 ,70 ) (Celsius)
R0          Temp: DMB OUT   Normal      40 Celsius (70 ,75 ,80 ,85 ) (Celsius)
R0          Temp: Yoda 0    Normal      54 Celsius (95 ,105,110,115) (Celsius)
R0          Temp: Yoda 1    Normal      62 Celsius (95 ,105,110,115) (Celsius)
R0          Temp: CPU Die   Normal      43 Celsius (100,110,120,125) (Celsius)
R0          Temp: FC FANS   Fan Speed 70% 26 Celsius (29 ,39 ,0 ) (Celsius)
R0          VDDC1: VX1      Normal      1005 mV      na
R0          VDDC1: VX2      Normal      7084 mV      na
R0          VDDC1: VX3      Normal      950 mV       na
R0          VDDC1: VP1      Normal      1800 mV      na
R0          VDDC1: VP2      Normal      2493 mV      na
R0          VDDC1: VP3      Normal      3325 mV      na
R0          VDDC1: VH        Normal      12019mV      na
R0          VDDC2: VX2      Normal      751 mV       na
R0          VDDC2: VX3      Normal      749 mV       na
R0          VDDC2: VX5      Normal      5076 mV      na
R0          VDDC2: VP1      Normal      1009 mV      na
R0          VDDC2: VP2      Normal      1008 mV      na
R0          VDDC2: VP3      Normal      1197 mV      na
R0          VDDC2: VP4      Normal      1514 mV      na
R0          VDDC2: VH        Normal      12003mV      na
R0          Temp: DDC IN    Normal      25 Celsius (55 ,65 ,75 ,80 ) (Celsius)
R0          Temp: DDC OUT   Normal      35 Celsius (75 ,85 ,95 ,100) (Celsius)
P0          Stby Vin       Normal      230 V AC     na
P0          Stby Iin       Normal      2 A         na
P0          Stby Vout      Normal      12 V DC     na
P0          Stby Iout      Normal      32 A         na
P0          Stby Temp1     Normal      24 Celsius (na ,na ,na ,na ) (Celsius)
P0          Stby Temp2     Normal      29 Celsius (na ,na ,na ,na ) (Celsius)
P0          Stby Temp3     Normal      35 Celsius (na ,na ,na ,na ) (Celsius)
R0          Stby VDMB1: VX1 Normal      1225 mV      na
R0          Stby VDMB1: VX2 Normal      6979 mV      na
R0          Stby VDMB1: VX3 Normal      1226 mV      na
R0          Stby VDMB1: VX4 Normal      999 mV       na
R0          Stby VDMB1: VP1 Normal      1791 mV      na
R0          Stby VDMB1: VP2 Normal      2560 mV      na
R0          Stby VDMB1: VP3 Normal      2558 mV      na
R0          Stby VDMB1: VP4 Normal      1050 mV      na
R0          Stby VDMB1: VH  Normal      11977mV      na
R0          Stby VDMB2: VX2 Normal      5005 mV      na
R0          Stby VDMB2: VX3 Normal      854 mV       na
R0          Stby VDMB2: VX4 Normal      878 mV       na
R0          Stby VDMB2: VX5 Normal      1008 mV      na
R0          Stby VDMB2: VP1 Normal      1789 mV      na
R0          Stby VDMB2: VP2 Normal      3312 mV      na
R0          Stby VDMB2: VH  Normal      11977mV      na
R0          Stby VDMB3: VX1 Normal      972 mV       na
R0          Stby VDMB3: VX2 Normal      1001 mV      na
R0          Stby VDMB3: VX5 Normal      5060 mV      na
R0          Stby VDMB3: VP1 Normal      2497 mV      na
R0          Stby VDMB3: VP2 Normal      1199 mV      na
R0          Stby VDMB3: VP3 Normal      1510 mV      na

```

show environment summary

```

R0          Stby VDMB3: VP4 Normal          1511 mV      na
R0          Stby VDMB3: VH Normal          11982mV      na
R0          Stby Temp: DMB INormal         22 Celsius (45 ,55 ,65 ,70 ) (Celsius)
R0          Stby Temp: DMB ONormal         32 Celsius (70 ,75 ,80 ,85 ) (Celsius)
R0          Stby Temp: Yoda Normal         43 Celsius (95 ,105,110,115) (Celsius)
R0          Stby Temp: Yoda Normal         45 Celsius (95 ,105,110,115) (Celsius)
R0          Stby Temp: CPU DNormal         33 Celsius (100,110,120,125) (Celsius)
R0          Stby Temp: FC FAFan Speed 70% 22 Celsius (29 ,39 ,0 ) (Celsius)
R0          Stby VDDC1: VX1 Normal         1005 mV      na
R0          Stby VDDC1: VX2 Normal         7070 mV      na
R0          Stby VDDC1: VX3 Normal         949 mV       na
R0          Stby VDDC1: VP1 Normal         1814 mV      na
R0          Stby VDDC1: VP2 Normal         2501 mV      na
R0          Stby VDDC1: VP3 Normal         3331 mV      na
R0          Stby VDDC1: VH Normal          11993mV      na
R0          Stby VDDC2: VX2 Normal         752 mV       na
R0          Stby VDDC2: VX3 Normal         750 mV       na
R0          Stby VDDC2: VX5 Normal         5052 mV      na
R0          Stby VDDC2: VP1 Normal         1009 mV      na
R0          Stby VDDC2: VP2 Normal         994 mV       na
R0          Stby VDDC2: VP3 Normal         1195 mV      na
R0          Stby VDDC2: VP4 Normal         1514 mV      na
R0          Stby VDDC2: VH Normal          11993mV      na
R0          Stby Temp: DDC INormal         22 Celsius (55 ,65 ,75 ,80 ) (Celsius)
R0          Stby Temp: DDC ONormal         28 Celsius (75 ,85 ,95 ,100) (Celsius)

```

show etherchannel summary

To show details on the ports, port-channel, and protocols in the controller, use the **show etherchannel summary** command.

show ethernet summary

This command has no arguments or keywords.

Command Default

None

Command Modes

Privileged Mode.

Command History

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

This example shows the details on the ports, port-channel, and protocols in the controller.

```
controller#show etherchannel summary
Flags:  D - down          P - bundled in port-channel
        I - stand-alone  s - suspended
        H - Hot-standby (LACP only)
        R - Layer3       S - Layer2
        U - in use       f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
```

```
Number of channel-groups in use: 2
Number of aggregators:          2
```

```
Group  Port-channel  Protocol  Ports
-----+-----+-----+-----
2      Po2 (SD)         -         -
23     Po23 (SD)        -         -
```

show fips authorization-key

To view the installed authorization key, use the **show fips authorization-key** command.

show fips authorization-key

Command Default None

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.12.1 | This command was introduced. |

This example shows how to view the installed authorization key:

```
Device# show fips authorization-key
FIPS: Stored key (16) : 12345678901234567890123456789012
```

show fips status

To view the status of FIPS on the device, use the **show fips status** command.

show fips status

Command Default

None

Command Modes

Privileged EXEC

Command History

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

This example shows how to view the status of FIPS on the device:

```
Device# show fips status  
Chassis is running in fips mode
```

show flash wipeout-log

To view the number of files, bytes deleted, free space and PID of the Access Point, use the **show flash wipeout-log** command.

show flash wipeout-log

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC (#)

| Command History | Release | Modification |
|-----------------|-----------------------------|------------------------------|
| | Cisco IOS XE Dublin 17.11.1 | This command was introduced. |

Usage Guidelines This command needs to be run on the AP console.

Examples The following example shows how to view the number of files, bytes deleted, free space and PID of the Access Point:

```
Device# show flash wipeout-log
```


show flexconnect office-extend diagnostics

To display the results of the network diagnostics for all flexconnect OfficeExtend AP, use the **show flexconnect office-extend diagnostics** command.

show flexconnect office-extend diagnostics

| | |
|---------------------------|--|
| Syntax Description | This command has no keywords or arguments. |
|---------------------------|--|

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

| | |
|----------------------|---------------------|
| Command Modes | Privileged EXEC (#) |
|----------------------|---------------------|

| Command History | Release | Modification |
|------------------------|-------------------------------|------------------------------|
| | Cisco IOS XE Bengaluru 17.5.1 | This command was introduced. |

| | |
|-------------------------|---|
| Usage Guidelines | To get periodic details for latency (current, minimum, or maximum) ensure that you enable link-latency under the ap profile, as given in the following example: |
|-------------------------|---|

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

If the above configuration is not in place, you will only see the following output:

```
Summary of OfficeExtend AP Link Latency

CAPWAP Latency Heartbeat

Current: current latency (ms)
Min: minimum latency (ms)
Max: maximum latency (ms)

Link Test

Upload: DTLS Upload (Mbps)
Latency: DTLS Link Latency (ms)
Jitter: DTLS Link Jitter (ms)

AP Name Last Latency Heartbeat from AP Current Max Min Last Link Test Run Upload Latency
Jitter
-----
ap-18 Disabled - - - 12/04/20 11:08:58 16 3
0
```

Examples

This following example shows how to display the network diagnostics information for OfficeExtend AP.

```
Device# show flexconnect office-extend diagnostics

Summary of OfficeExtend AP Link Latency

CAPWAP Latency Heartbeat

Current: current latency (ms)
```

show flexconnect office-extend diagnostics

Min: minimum latency (ms)
Max: maximum latency (ms)

Link Test

Upload: DTLS Upload (Mbps)
Latency: DTLS Link Latency (ms)
Jitter: DTLS Link Jitter (ms)

| AP Name | Last Latency | Heartbeat from AP | Current | Max | Min | Last Link Test | Run | Upload | Latency |
|---------|-------------------|-------------------|---------|-----|-----|-------------------|-----|--------|---------|
| ap-18 | 1 minute 1 second | | 0 | 0 | 0 | 12/04/20 09:19:48 | 8 | | 2 |

show flow exporter

To display flow exporter status and statistics, use the **show flow exporter** command in privileged EXEC mode.

```
show flow exporter [{export-ids netflow-v9|[name] exporter-name [{statistics|templates}]]|statistics|templates}]
```

| Syntax Description | |
|------------------------------|---|
| export-ids netflow-v9 | (Optional) Displays the NetFlow Version 9 export fields that can be exported and their IDs. |
| name | (Optional) Specifies the name of a flow exporter. |
| <i>exporter-name</i> | (Optional) Name of a flow exporter that was previously configured. |
| statistics | (Optional) Displays statistics for all flow exporters or for the specified flow exporter. |
| templates | (Optional) Displays template information for all flow exporters or for the specified flow exporter. |

Command Default None

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

The following example displays the status and statistics for all of the flow exporters configured on a device:

```
Device# show flow exporter
Flow Exporter FLOW-EXPORTER-1:
  Description:           Exports to the datacenter
  Export protocol:       NetFlow Version 9
  Transport Configuration:
    Destination IP address: 192.168.0.1
    Source IP address:     192.168.0.2
    Transport Protocol:    UDP
    Destination Port:      9995
    Source Port:           55864
    DSCP:                  0x0
    TTL:                   255
    Output Features:       Used
```

This table describes the significant fields shown in the display:

Table 1: show flow exporter Field Descriptions

| Field | Description |
|---------------|--|
| Flow Exporter | The name of the flow exporter that you configured. |

| Field | Description |
|-------------------------|--|
| Description | The description that you configured for the exporter, or the default description User defined. |
| Transport Configuration | The transport configuration fields for this exporter. |
| Destination IP address | The IP address of the destination host. |
| Source IP address | The source IP address used by the exported packets. |
| Transport Protocol | The transport layer protocol used by the exported packets. |
| Destination Port | The destination UDP port to which the exported packets are sent. |
| Source Port | The source UDP port from which the exported packets are sent. |
| DSCP | The differentiated services code point (DSCP) value. |
| TTL | The time-to-live value. |
| Output Features | Specifies whether the output-features command, which causes the output features to be run on Flexible NetFlow export packets, has been used or not. |

The following example displays the status and statistics for all of the flow exporters configured on a device:

```
Device# show flow exporter name FLOW-EXPORTER-1 statistics
Flow Exporter FLOW-EXPORTER-1:
  Packet send statistics (last cleared 2w6d ago):
    Successfully sent:      0                (0 bytes)
```

show flow interface

To display the configuration and status for an interface, use the **show flow interface** command in privileged EXEC mode.

show flow interface [*type number*]

Syntax Description

type (Optional) The type of interface on which you want to display accounting configuration information.

number (Optional) The number of the interface on which you want to display accounting configuration information.

Command Modes

Privileged EXEC

Command History

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

Examples

The following example displays the accounting configuration on Ethernet interfaces 0/0 and 0/1:

```
Device# show flow interface gigabitethernet1/0/1

Interface Ethernet1/0
  monitor:          FLOW-MONITOR-1
  direction:       Output
  traffic(ip):     on
Device# show flow interface gigabitethernet1/0/2
Interface Ethernet0/0
  monitor:          FLOW-MONITOR-1
  direction:       Input
  traffic(ip):     sampler SAMPLER-2#
```

The table below describes the significant fields shown in the display.

Table 2: show flow interface Field Descriptions

| Field | Description |
|------------|--|
| Interface | The interface to which the information applies. |
| monitor | The name of the flow monitor that is configured on the interface. |
| direction: | The direction of traffic that is being monitored by the flow monitor. The possible values are: <ul style="list-style-type: none"> • Input—Traffic is being received by the interface. • Output—Traffic is being transmitted by the interface. |

| Field | Description |
|-------------|--|
| traffic(ip) | <p data-bbox="467 296 1162 323">Indicates if the flow monitor is in normal mode or sampler mode.</p> <p data-bbox="467 342 724 369">The possible values are:</p> <ul data-bbox="505 388 1474 499" style="list-style-type: none"><li data-bbox="505 388 964 415">• on—The flow monitor is in normal mode.<li data-bbox="505 438 1474 499">• sampler—The flow monitor is in sampler mode (the name of the sampler will be included in the display). |

show flow monitor

To display the status and statistics for a flow monitor, use the **show flow monitor** command in privileged EXEC mode.

| Syntax Description | name | (Optional) Specifies the name of a flow monitor. |
|--------------------|---------------------|--|
| | <i>monitor-name</i> | (Optional) Name of a flow monitor that was previously configured. |
| | cache | (Optional) Displays the contents of the cache for the flow monitor. |
| | format | (Optional) Specifies the use of one of the format options for formatting the display output. |
| | csv | (Optional) Displays the flow monitor cache contents in comma-separated variables (CSV) format. |
| | record | (Optional) Displays the flow monitor cache contents in record format. |
| | table | (Optional) Displays the flow monitor cache contents in table format. |
| | statistics | (Optional) Displays the statistics for the flow monitor. |

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

Usage Guidelines The **cache** keyword uses the record format by default.

The uppercase field names in the display output of the **show flowmonitor monitor-name cache** command are key fields that uses to differentiate flows. The lowercase field names in the display output of the **show flow monitor monitor-name cache** command are nonkey fields from which collects values as additional data for the cache.

Examples

The following example displays the status for a flow monitor:

```
Device# show flow monitor FLOW-MONITOR-1

Flow Monitor FLOW-MONITOR-1:
  Description:      Used for basic traffic analysis
  Flow Record:     flow-record-1
  Flow Exporter:   flow-exporter-1
                  flow-exporter-2

Cache:
  Type:            normal
  Status:         allocated
  Size:           4096 entries / 311316 bytes
  Inactive Timeout: 15 secs
  Active Timeout: 1800 secs
```

This table describes the significant fields shown in the display.

Table 3: show flow monitor monitor-name Field Descriptions

| Field | Description |
|------------------|---|
| Flow Monitor | Name of the flow monitor that you configured. |
| Description | Description that you configured or the monitor, or the default description User defined. |
| Flow Record | Flow record assigned to the flow monitor. |
| Flow Exporter | Exporters that are assigned to the flow monitor. |
| Cache | Information about the cache for the flow monitor. |
| Type | Flow monitor cache type. The value is always normal, as it is the only supported cache type. |
| Status | Status of the flow monitor cache. The possible values are: <ul style="list-style-type: none"> • allocated—The cache is allocated. • being deleted—The cache is being deleted. • not allocated—The cache is not allocated. |
| Size | Current cache size. |
| Inactive Timeout | Current value for the inactive timeout in seconds. |
| Active Timeout | Current value for the active timeout in seconds. |

The following example displays the status, statistics, and data for the flow monitor named FLOW-MONITOR-1:

This table describes the significant fields shown in the display.

The following example displays the status, statistics, and data for the flow monitor named FLOW-MONITOR-1 in a table format:

The following example displays the status, statistics, and data for the flow monitor named FLOW-MONITOR-IPv6 (the cache contains IPv6 data) in record format:

The following example displays the status and statistics for a flow monitor:

show flow record

To display the status and statistics for a flow record, use the **show flow record** command in privileged EXEC mode.

```
show flow record [{name] record-name}]
```

| | |
|---------------------------|--|
| Syntax Description | name (Optional) Specifies the name of a flow record. |
| | <i>record-name</i> (Optional) Name of a user-defined flow record that was previously configured. |
| Command Default | None |
| Command Modes | Privileged EXEC |
| Command History | Release |
| | Modification |
| | Cisco IOS XE Gibraltar 16.10.1 This command was introduced. |

The following example displays the status and statistics for FLOW-RECORD-1:

```
Device# show flow record FLOW-RECORD-1
flow record FLOW-RECORD-1:
  Description:      User defined
  No. of users:    0
  Total field space: 24 bytes
  Fields:
    match ipv6 destination address
    match transport source-port
    collect interface input
```

show flow record wireless avc basic

To view information about the flow records for wireless avc basic, use the **show flow record wireless avc basic** command.

show flow record wireless avc basic

| | | |
|---------------------------|--|------------------------------|
| 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. |

Example

The following example shows how to see information about the flow records for wireless avc basic:

```
Device# show flow record wireless avc basic

flow record wireless avc basic:
  Description:          Basic Wireless AVC template
  No. of users:         1
  Total field space:   78 bytes
  Fields:
    match ipv4 protocol
    match ipv4 source address
    match ipv4 destination address
    match transport source-port
    match transport destination-port
    match flow direction
    match application name
    match wireless ssid
    collect counter bytes long
    collect counter packets long
    collect wireless ap mac address
    collect wireless client mac address
```

show flow record wireless avc ipv6 basic

To view information about the flow records for wireless avc ipv6 basic, use the **show flow record wireless avc ipv6 basic** command.

show flow record wireless avc ipv6 basic

| | | |
|---------------------------|--|------------------------------|
| 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. |

Example

The following example shows how to see information about the flow records for wireless avc ipv6 basic:

```
Device# show flow record wireless avc ipv6 basic

flow record wireless avc ipv6 basic:
  Description:          Ipv6 Wireless AVC flow template
  No. of users:         1
  Total field space:   102 bytes
  Fields:
    match ipv6 protocol
    match ipv6 source address
    match ipv6 destination address
    match transport source-port
    match transport destination-port
    match flow direction
    match wireless ssid
    collect counter bytes long
    collect counter packets long
    collect application name
    collect wireless ap mac address
    collect wireless client mac address
```

show gnxi state

To verify the gnxi details, use the **show gnxi state** command.

show gnxi state

| | | |
|---------------------------|-------------------------------|---|
| Syntax Description | detail | Displays the gnxi detailed state. |
| | stats | Displays the gnxi operational statistics. |
| Command Default | None | |
| Command Modes | Privileged EXEC | |
| Command History | Release | Modification |
| | Cisco IOS XE Bengaluru 17.6.1 | This command was introduced. |

The following example shows how to verify the gnxi details:

```
Device# show gnxi state detail
Settings
=====
Server: Enabled
Server port: 50052
Secure server: Disabled
Secure server port: 5000
Secure client authentication: Enabled
Secure trustpoint: test
Secure client trustpoint:
Secure password authentication: Disabled

GNMI
====
Admin state: Enabled
Oper status: Up
State: Provisioned

gRPC Server
-----
Admin state: Enabled
Oper status: Up

Configuration service
-----
Admin state: Enabled
Oper status: Up

Telemetry service
-----
Admin state: Enabled
Oper status: Up

GNOI
```

```
====
```

```
Cert Management service
```

```
-----
```

```
Admin state: Enabled
```

```
Oper status: Up
```

```
OS Image service
```

```
-----
```

```
Admin state: Disabled
```

```
Oper status: Up
```

```
Supported: Not supported on this platform
```

show history channel interface dot11Radio all

To check channel change or trigger reason and history, use the **show history channel interface dot11Radio all** command.

show history channel interface dot11Radio all

| | | |
|---------------------------|--|------------------------------|
| Syntax Description | This command has no keywords or arguments. | |
| Command Default | None | |
| Command Modes | Privileged EXEC (#) | |
| Command History | Release | Modification |
| | Cisco IOS XE Amsterdam 17.2.1 | This command was introduced. |

Examples

This example shows how to check channel change or trigger reason and history:

```
Device# show history channel interface dot11Radio all

          Timestamp Slot Client count Channel Trigger
Fri May 31 12:57:04 2019    0         0      11 RRM-DCA
Fri May 31 13:10:02 2019    0         0       1 RRM-DCA
Fri May 31 12:57:04 2019    1         0       60 Manual
Fri May 31 13:00:16 2019    1         0      149   DFS
```

show interfaces

To display the administrative and operational status of all interfaces or for a specified interface, use the **show interfaces** command in privileged EXEC mode.

```
show interfaces [{interface-id | vlan vlan-id}] [{accounting | capabilities [module number] | debounce
| description | etherchannel | flowcontrol | private-vlan mapping | pruning | stats | status [{err-disabled}]
| trunk}]
```

| Syntax | Description |
|-----------------------------|--|
| <i>interface-id</i> | (Optional) ID of the interface. Valid interfaces include physical ports (including type, stack member, module, and port number) and port channels. The port channel range is 1 to 48. |
| vlan <i>vlan-id</i> | (Optional) VLAN identification. The range is 1 to 4094. |
| accounting | (Optional) Displays accounting information on the interface, including active protocols and input and output packets and octets. Note The display shows only packets processed in software; hardware-switched packets do not appear. |
| capabilities | (Optional) Displays the capabilities of all interfaces or the specified interface, including the features and options that you can configure on the interface. Though visible in the command line help, this option is not available for VLAN IDs. |
| module <i>number</i> | (Optional) Displays capabilities of all interfaces on the switch or specified stack member. This option is not available if you entered a specific interface ID. |
| description | (Optional) Displays the administrative status and description set for an interface. |
| etherchannel | (Optional) Displays interface EtherChannel information. |
| flowcontrol | (Optional) Displays interface flow control information. |
| private-vlan mapping | (Optional) Displays private-VLAN mapping information for the VLAN switch virtual interfaces (SVIs). This keyword is not available if the switch is running the LAN base feature set. |
| pruning | (Optional) Displays trunk VTP pruning information for the interface. |
| stats | (Optional) Displays the input and output packets by switching the path for the interface. |
| status | (Optional) Displays the status of the interface. A status of unsupported in the Type field means that a non-Cisco small form-factor pluggable (SFP) module is inserted in the module slot. |

| | |
|---------------------|--|
| err-disabled | (Optional) Displays interfaces in an error-disabled state. |
| trunk | (Optional) Displays interface trunk information. If you do not specify an interface, only information for active trunking ports appears. |



Note Though visible in the command-line help strings, the **crb**, **fair-queue**, **irb**, **mac-accounting**, **precedence**, **random-detect**, **rate-limit**, and **shape** keywords are not supported.

Command Default None

Command Modes Privileged EXEC

| Command History | Release | Modification |
|------------------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

Usage Guidelines

The **show interfaces capabilities** command with different keywords has these results:

- Use the **show interface capabilities module *number*** command to display the capabilities of all interfaces on that chassis in the stack. If there is no chassis with that module number in the stack, there is no output.
- Use the **show interfaces *interface-id* capabilities** to display the capabilities of the specified interface.
- Use the **show interfaces capabilities** (with no module number or interface ID) to display the capabilities of all interfaces in the stack.

This is an example of output from the **show interfaces** command for an interface on stack member 3:

```
Device# show interfaces gigabitethernet3/0/2
GigabitEthernet3/0/2 is down, line protocol is down (notconnect)
  Hardware is Gigabit Ethernet, address is 2037.064d.4381 (bia 2037.064d.4381)
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, Auto-speed, media type is 10/100/1000BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts (0 multicasts)
    0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 0 multicast, 0 pause input
    0 input packets with dribble condition detected
    0 packets output, 0 bytes, 0 underruns
```



```

0 output errors, 0 collisions, 1 interface resets
0 unknown protocol drops
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier, 0 pause output
0 output buffer failures, 0 output buffers swapped out

```

This is an example of output from the **show interfaces interface description** command when the interface has been described as *Connects to Marketing* by using the **description** interface configuration command:

```

Device# show interfaces gigabitethernet1/0/2 description
Interface          Status      Protocol Description
Gi1/0/2            up          down       Connects to Marketing

```

This is an example of output from the **show interfaces interface-id pruning** command when pruning is enabled in the VTP domain:

```

Device# show interfaces gigabitethernet1/0/2 pruning
Port      Vlans pruned for lack of request by neighbor
Gi1/0/2   3,4

Port      Vlans traffic requested of neighbor
Gi1/0/2   1-3

```

This is an example of output from the **show interfaces stats** command for a specified VLAN interface:

```

Device# show interfaces vlan 1 stats
Switching path  Pkts In   Chars In   Pkts Out   Chars Out
Processor       1165354   136205310  570800     91731594
Route cache     0         0          0          0
Total          1165354   136205310  570800     91731594

```

These are examples of output from the **show interfaces status** command for a specific interface when private VLANs are configured. Port 22 is configured as a private-VLAN host port. It is associated with primary VLAN 20 and secondary VLAN 25:

```

Device# show interfaces gigabitethernet1/0/22 status
Port   Name      Status      Vlan      Duplex  Speed  Type
Gi1/0/22      connected  20,25      a-full    a-100   10/100BaseTX

```

In this example, port 20 is configured as a private-VLAN promiscuous port. The display shows only the primary VLAN 20:

```

Device# show interfaces gigabitethernet1/0/20 status
Port   Name      Status      Vlan      Duplex  Speed  Type
Gi1/0/20      connected  20         a-full    a-100   10/100BaseTX

```

This is an example of output from the **show interfaces status err-disabled** command. It displays the status of interfaces in the error-disabled state:

```

Device# show interfaces status err-disabled
Port   Name      Status      Reason
Gi1/0/2      err-disabled  gbic-invalid
Gi2/0/3      err-disabled  dtp-flap

```

This is an example of output from the **show interfaces interface-id pruning** command:

```
Device# show interfaces gigabitethernet1/0/2 pruning
Port Vlans pruned for lack of request by neighbor
```

```
Device# show interfaces gigabitethernet1/0/1 trunk
Port      Mode      Encapsulation  Status      Native vlan
Gi1/0/1   on        802.1q         other       10

Port      Vlans allowed on trunk
Gi1/0/1   none

Port      Vlans allowed and active in management domain
Gi1/0/1   none

Port      Vlans in spanning tree forwarding state and not pruned
Gi1/0/1   none
```

show interfaces dot11Radio asr-info

To view advanced scheduling request statistics along with advanced scheduling request capability and uplink latency statistics for advanced scheduling request clients on a WLAN, use the **show interfaces dot11Radio asr-info** command.

```
show interfaces dot11Radio asr-info radio-interface-number { all | mac-address }
```

| Syntax Description | | | | | |
|-------------------------------|--|---------|--------------|-------------------------------|-----------------------------|
| <i>radio-interface-number</i> | Interface number for 802.11 radio. | | | | |
| all | Displays advanced scheduling request statistics along with advanced scheduling request capability and uplink latency statistics for all the advanced scheduling request clients on a WLAN. | | | | |
| <i>mac-address</i> | MAC address of the AP. | | | | |
| Command Default | None | | | | |
| Command Modes | Privileged EXEC (#) | | | | |
| Command History | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Bengaluru 17.4.1</td> <td>This command was introduced</td> </tr> </tbody> </table> | Release | Modification | Cisco IOS XE Bengaluru 17.4.1 | This command was introduced |
| Release | Modification | | | | |
| Cisco IOS XE Bengaluru 17.4.1 | This command was introduced | | | | |

Examples

The following example shows how to view advanced scheduling request statistics along with advanced scheduling request capability and uplink latency statistics for all the advanced scheduling request clients on a WLAN:

```
Device# show interfaces dot11Radio 1 asr-info all

[*10/12/2020 18:45:21.0149]
[*10/12/2020 18:45:21.0150] Client-MAC:[26:52:CF:C8:D0:1C] AID:[3] ASR-Capability:[0x1]
[*10/12/2020 18:45:21.0150] BE- LAT[0-20]:[267] LAT[20-40]:[57] LAT[40-100]:[32]
LAT[>100]:[26]
[*10/12/2020 18:45:21.0150] BK- LAT[0-20]:[0] LAT[20-40]:[0] LAT[40-100]:[0] LAT[>100]:[0]
[*10/12/2020 18:45:21.0150] VI- LAT[0-20]:[0] LAT[20-40]:[0] LAT[40-100]:[0] LAT[>100]:[0]
[*10/12/2020 18:45:21.0150] VO- LAT[0-20]:[2222] LAT[20-40]:[409] LAT[40-100]:[224]
LAT[>100]:[163]
[*10/12/2020 18:45:21.0150]
[*10/12/2020 18:45:21.0206] HTT_PEER_DETAILS_TLV:
[*10/12/2020 18:45:21.0206] peer_type = 0
[*10/12/2020 18:45:21.0206] sw_peer_id = 98
[*10/12/2020 18:45:21.0206] vdev_id = 25
[*10/12/2020 18:45:21.0206] pdev_id = 0
[*10/12/2020 18:45:21.0206] ast_idx = 1187
[*10/12/2020 18:45:21.0206] mac_addr = 26:52:cf:c8:d0:1c
[*10/12/2020 18:45:21.0206] peer_flags = 0x200006f9
[*10/12/2020 18:45:21.0206] qpeer_flags = 0x8
[*10/12/2020 18:45:21.0206]
[*10/12/2020 18:45:21.0206] HTT_STATS_PEER_ASR_STATS_TLV
[*10/12/2020 18:45:21.0206] asr_bmap: 0x8
[*10/12/2020 18:45:21.0206] asr_muedca_update_cnt: 1
[*10/12/2020 18:45:21.0206] asr_muedca_reset_cnt: 1
```

show interfaces dot11Radio asr-info

```
[*10/12/2020 18:45:21.0206] asr_ul_mu_bsr_trigger: 2376
[*10/12/2020 18:45:21.0206] asr_min_trig_intv- BE:0          BK:0 VI:0 VO:19
[*10/12/2020 18:45:21.0206] asr_max_trig_intv- BE:0          BK:0 VI:0 VO:20
[*10/12/2020 18:45:21.0207] asr_min_alloc_rate- BE:0         BK:0 VI:0 VO:12
[*10/12/2020 18:45:21.0207] asr_ul_su_data_ppdu_cnt- BE:0     BK:0 VI:0 VO:2149
[*10/12/2020 18:45:21.0207] asr_ul_su_data_ppdu_bytes- BE:0   BK:0 VI:0 VO:757546
[*10/12/2020 18:45:21.0207] asr_ul_mu_trig_ppdu_cnt- BE:0     BK:0 VI:0 VO:5002
[*10/12/2020 18:45:21.0207] asr_ul_mu_trig_ppdu_bytes- BE:0   BK:0 VI:0 VO:2400960
[*10/12/2020 18:45:21.0207] asr_ul_mu_data_ppdu_cnt- BE:0     BK:0 VI:0 VO:2134
[*10/12/2020 18:45:21.0207] asr_ul_mu_data_ppdu_bytes- BE:0   BK:0 VI:0 VO:736578
[*10/12/2020 18:45:21.0207] asr_ul_mu_data_padding_bytes- BE:0 BK:0 VI:0 VO:2953488
```

show interfaces wired

To view the wired interface details, use the **show interfaces wired** command.

show interfaces wired *wired-interface-number*

Syntax Description

wired-interface-number Wired interface number.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

| Release | Modification |
|-------------------------------|------------------------------|
| Cisco IOS XE Amsterdam 17.2.1 | This command was introduced. |

Examples

This example shows how to view the wired interface details:

```
Device# show interfaces wired 0

wired0    Link encap:Ethernet  HWaddr C8:8B:5E:BA:D0 eMac Status: UP
          inet addr:20.200.51.14  Bcast:20.255.255.255  Mask:255.255.255.255
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:2400  Metric:1
          full Duplex, 1000 Mb/s

Wired0 Port Statistics:
ID        :                2          TYPE        :                0
RX PKTS   :            35109/431     TX PKTS     :            1307/11
RX OCTETS :           2899435/34925   TX OCTETS   :           377424/1575
RX ERR    :                287/0     TX ERR      :                0/0
```

show inventory

To display the product inventory listing of all Cisco products installed in the networking device, use the **show inventory** command.

```
show inventory [ entity-name | [ fru | oid | raw ] entity-name ]
```

| Syntax Description | |
|--------------------|--|
| <i>entity-name</i> | (Optional) Name of a Cisco entity (for example, chassis, backplane, module, or slot). A quoted string may be used to display very specific UDI information; for example "sfslot 1" shows the UDI information for slot 1 of an entity named sfslot. |
| fru | (Optional) To display the component details of the fru entities within the container hierarchy in Cisco products. |
| oid | (Optional) To display the vendor specific hardware registration number for each part of the device. |
| raw | (Optional) To view the information about all Cisco products—referred to as entities—installed in the Cisco networking device, even if the entities do not have a product ID (PID) value, a unique device identifier (UDI), or other physical identification. |

Command Default None

Command Modes Privileged EXEC (#)

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

Usage Guidelines The **show inventory** command retrieves and displays inventory information about each Cisco product in the form of a UDI. The UDI is a combination of three separate data elements: a product identifier (PID), a version identifier (VID), and the serial number (SN).

The PID is the name by which the product can be ordered; it has been historically called the "Product Name" or "Part Number." This is the identifier that one would use to order an exact replacement part.

The VID is the version of the product. Whenever a product has been revised, the VID will be incremented. The VID is incremented according to a rigorous process derived from Telcordia GR-209-CORE, an industry guideline that governs product change notices.

The SN is the vendor-unique serialization of the product. Each manufactured product will carry a unique serial number assigned at the factory, which cannot be changed in the field. This is the means by which to identify an individual, specific instance of a product.

The UDI refers to each product as an entity. Some entities, such as a chassis, will have subentities like slots. Each entity will display on a separate line in a logically ordered presentation that is arranged hierarchically by Cisco entities.

Use the **show inventory** command without options to display a list of Cisco entities installed in the networking device that are assigned a PID.

Examples

This example shows how to display the product inventory listing of a Cisco product installed in the networking device:

```
Device# show inventory
```

```
NAME: "module R0", DESCR: "Cisco C9800-CL Route Processor"
```

```
PID: C9800-CL-K9 , VID: V00 , SN: Jxx1xxxxx1x
```

show ip

To view the IP information, use the **show ip** command.

| Syntax | Description |
|-------------------------|---|
| access-lists | Lists the IP access lists |
| interface | Displays the IP interface status and configuration |
| brief | Displays the brief summary of IP status and configuration |
| route | Displays the IP routing table |
| tunnel | Displays the IP tunnel information |
| eogre | Displays the EoGRE tunnel information |
| domain | Displays the EoGRE tunnel domain information |
| forwarding-table | Displays the EoGRE tunnel encapsulation and decapsulation information |
| gateway | Displays the EoGRE tunnel gateway information |
| fabric | Displays the IP fabric tunnel information |
| summary | Displays the information for all tunnels |

| Command Modes |
|---------------------|
| User EXEC (>) |
| Privileged EXEC (#) |

| Command History | Release | Modification |
|-----------------|-----------|------------------------------|
| | 8.1.111.0 | This command was introduced. |

The following example shows how to view information about the lists the IP access lists:

```
cisco-wave2-ap# show ip access-lists
```


show ip igmp snooping igmpv2-tracking

To display group and IP address entries, use the **show ip igmp snooping igmpv2-tracking** command in privileged EXEC mode.



Note The command displays group and IP address entries only for wireless multicast IGMP joins and not for wired joins. This command also displays output only if wireless multicast is enabled.

show ip igmp snooping igmpv2-tracking

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

show ip igmp snooping querier

To display the configuration and operation information for the IGMP querier that is configured on a device, use the **show ip igmp snooping querier** command in user EXEC mode.

show ip igmp snooping querier [**vlan** *vlan-id*] [**detail**]

| | |
|---------------------------|---|
| Syntax Description | vlan <i>vlan-id</i> (Optional) Specifies a VLAN; Ranges are from 1—1001 and 1006—4094. |
| | detail (Optional) Displays detailed IGMP querier information. |

| | |
|----------------------|------------------------------|
| Command Modes | User EXEC Privileged EXEC |
|----------------------|------------------------------|

| | | |
|------------------------|--------------------------------|------------------------------|
| Command History | Release | Modification |
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

Usage Guidelines Use the **show ip igmp snooping querier** command to display the IGMP version and the IP address of a detected device, also called a querier, that sends IGMP query messages. A subnet can have multiple multicast routers but only one IGMP querier. In a subnet running IGMPv2, one of the multicast routers is elected as the querier. The querier can be a Layer 3 device.

The **show ip igmp snooping querier** command output also shows the VLAN and the interface on which the querier was detected. If the querier is the device, the output shows the Port field as Router. If the querier is a router, the output shows the port number on which the querier was detected in the Port field.

The **show ip igmp snooping querier detail** user EXEC command is similar to the **show ip igmp snooping querier** command. However, the **show ip igmp snooping querier** command displays only the device IP address most recently detected by the device querier.

The **show ip igmp snooping querier detail** command displays the device IP address most recently detected by the device querier and this additional information:

- The elected IGMP querier in the VLAN
- The configuration and operational information pertaining to the device querier (if any) that is configured in the VLAN

Expressions are case sensitive, for example, if you enter | **exclude output**, the lines that contain "output" do not appear, but the lines that contain "Output" appear.

Examples

The following is a sample output from the **show ip igmp snooping querier** command:

```
Device> show ip igmp snooping querier
Vlan      IP Address      IGMP Version      Port
-----
1         172.20.50.11    v3                 Gi1/0/1
2         172.20.40.20    v2                 Router
```

The following is a sample output from the **show ip igmp snooping querier detail** command:

```
Device> show ip igmp snooping querier detail
```

```
Vlan      IP Address      IGMP Version  Port
-----
1         10.0.0.10      v2           Fa8/0/1
Global IGMP device querier status
```

```
-----
admin state           : Enabled
admin version        : 2
source IP address     : 0.0.0.0
query-interval (sec) : 60
max-response-time (sec) : 10
querier-timeout (sec) : 120
tcn query count      : 2
tcn query interval (sec) : 10
Vlan 1: IGMP device querier status
```

```
-----
elected querier is 10.0.0.10      on port Fa8/0/1
-----
```

```
admin state           : Enabled
admin version        : 2
source IP address     : 10.1.1.65
query-interval (sec) : 60
max-response-time (sec) : 10
querier-timeout (sec) : 120
tcn query count      : 2
tcn query interval (sec) : 10
operational state     : Non-Querier
operational version   : 2
tcn query pending count : 0
```

show ip igmp snooping wireless mcast-spi-count

To display the statistics of the number of multicast stateful packet inspections (SPIs) per multicast group ID (MGID) sent to the device, use the **show ip igmp snooping wireless mcast-spi-count** command in privileged EXEC mode.

show ip igmp snooping wireless mcast-spi-count

This command has no arguments or keywords.

Command Default None

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

Usage Guidelines None

Examples

This is an example of output from the **show ip igmp snooping wireless mcast-spi-count** command:

```
Device# show ip igmp snooping wireless mcast-spi-count

Stats for Mcast Client Add/Delete SPI Messages Sent to WCM

MGID      ADD MSGs      Del MSGs
-----
4160      1323          667
```

show ip igmp snooping wireless mgid

To display multicast group ID (MGID) mappings, use the **show ip igmp snooping wireless mgid** command in privileged EXEC mode.

show ip igmp snooping wireless mgid

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

Usage Guidelines None

Examples

This is an example of output from the **show ip igmp snooping wireless mgid** command:

```
Device# show ip igmp snooping wireless mgid

Total number of L2-MGIDs      = 0

Total number of MCAST MGIDs = 0

Wireless multicast is Enabled in the system
Vlan    bcast    nonip-mcast    mcast    mgid    Stdby Flags
1       Disabled  Disabled      Enabled   Disabled 0:0:1:0
25      Disabled  Disabled      Enabled   Disabled 0:0:1:0
34      Disabled  Disabled      Enabled   Disabled 0:0:1:0
200     Disabled  Disabled      Enabled   Disabled 0:0:1:0
1002    Enabled   Enabled       Enabled   Disabled 0:0:1:0
1003    Enabled   Enabled       Enabled   Disabled 0:0:1:0
1004    Enabled   Enabled       Enabled   Disabled 0:0:1:0
1005    Enabled   Enabled       Enabled   Disabled 0:0:1:0

Index  MGID                               (S, G, V)
-----
```

show ip nbar protocol-discovery wlan

To see NBAR protocol discovery statistics for a WLAN, use the **show ip nbar protocol-discovery wlan** command.

show ip nbar protocol-discovery wlan *wlan-name*

| | | |
|---------------------------|--------------------------------|---|
| Syntax Description | <i>wlan-name</i> | Name of the WLAN. |
| Command Default | None | |
| Command Modes | Privileged EXEC | |
| Command History | Release | Modification |
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

Examples

The following example shows how to see the NBAR protocol discovery statistics for a WLAN named *mywlan*:

```
Device# show ip nbar protocol-discovery wlan mywlan
```

show ipv6 access-list

To display the contents of all current IPv6 access lists, use the **show ipv6 access-list** command in user EXEC or privileged EXEC mode.

```
show ipv6 access-list [access-list-name]
```

| | |
|---------------------------|---|
| Syntax Description | <i>access-list-name</i> (Optional) Name of access list. |
|---------------------------|---|

| | |
|------------------------|--------------------------------------|
| Command Default | All IPv6 access lists are displayed. |
|------------------------|--------------------------------------|

| | |
|----------------------|------------------------------|
| Command Modes | User EXEC Privileged EXEC |
|----------------------|------------------------------|

Command History

| Command History | Release | Modification |
|-----------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

| | |
|-------------------------|--|
| Usage Guidelines | The show ipv6 access-list command provides output similar to the show ip access-list command, except that it is IPv6-specific. |
|-------------------------|--|

Examples

The following output from the **show ipv6 access-list** command shows IPv6 access lists named inbound, tcptraffic, and outbound:

```
Device# show ipv6 access-list
IPv6 access list inbound
  permit tcp any any eq bgp reflect tcptraffic (8 matches) sequence 10
  permit tcp any any eq telnet reflect tcptraffic (15 matches) sequence 20
  permit udp any any reflect udptraffic sequence 30
IPv6 access list tcptraffic (reflexive) (per-user)
  permit tcp host 2001:0DB8:1::1 eq bgp host 2001:0DB8:1::2 eq 11000 timeout 300 (time
    left 243) sequence 1
  permit tcp host 2001:0DB8:1::1 eq telnet host 2001:0DB8:1::2 eq 11001 timeout 300
    (time left 296) sequence 2
IPv6 access list outbound
  evaluate udptraffic
  evaluate tcptraffic
```

The following sample output shows IPv6 access list information for use with IPsec:

```
Device# show ipv6 access-list
IPv6 access list Tunnel0-head-0-ACL (crypto)
  permit ipv6 any any (34 matches) sequence 1
IPv6 access list Ethernet2/0-ipsecv6-ACL (crypto)
  permit 89 FE80::/10 any (85 matches) sequence 1
```

The table below describes the significant fields shown in the display.

Table 4: show ipv6 access-list Field Descriptions

| Field | Description |
|--------------------------|--|
| ipv6 access list inbound | Name of the IPv6 access list, for example, inbound. |
| permit | Permits any packet that matches the specified protocol type. |
| tcp | Transmission Control Protocol. The higher-level (Layer 4) protocol type that the packet must match. |
| any | Equal to ::/0. |
| eq | An equal operand that compares the source or destination ports of TCP or UDP packets. |
| bgp | Border Gateway Protocol. The lower-level (Layer 3) protocol type that the packet must be equal to. |
| reflect | Indicates a reflexive IPv6 access list. |
| tcptraffic (8 matches) | The name of the reflexive IPv6 access list and the number of matches for the access list. The clear ipv6 access-list privileged EXEC command resets the IPv6 access list match counters. |
| sequence 10 | Sequence in which an incoming packet is compared to lines in an access list. Lines in an access list are ordered from first priority (lowest number, for example, 10) to last priority (highest number, for example, 80). |
| host 2001:0DB8:1::1 | The source IPv6 host address that the source address of the packet must match. |
| host 2001:0DB8:1::2 | The destination IPv6 host address that the destination address of the packet must match. |
| 11000 | The ephemeral source port number for the outgoing connection. |
| timeout 300 | The total interval of idle time (in seconds) after which the temporary IPv6 reflexive access list named tcptraffic will time out for the indicated session. |
| (time left 243) | The amount of idle time (in seconds) remaining before the temporary IPv6 reflexive access list named tcptraffic is deleted for the indicated session. Additional received traffic that matches the indicated session resets this value to 300 seconds. |
| evaluate udptraffic | Indicates the IPv6 reflexive access list named udptraffic is nested in the IPv6 access list named outbound. |

show ipv6 hop-by-hop status

To display information about IPv6 hop-by-hop header processing, use the **show ipv6 hop-by-hop status** command.

show ipv6 hop-by-hop status

| | | |
|---------------------------|--|------------------------------|
| Syntax Description | This command has no arguments or keywords. | |
| Command Default | None | |
| Command Modes | Privileged EXEC (#) | |
| Command History | Release | Modification |
| | Cisco IOS XE Bengaluru 17.6.1 | This command was introduced. |

Examples

The following example displays information about IPv6 hop-by-hop header processing:

```
Device# show ipv6 hop-by-hop status
```

show ipv6 mld snooping

Use the **show ipv6 mld snooping** command in EXEC mode to display IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping configuration of the switch or the VLAN.

show ipv6 mld snooping [**vlan** *vlan-id*]

| Syntax Description | vlan | <i>vlan-id</i> | (Optional) Specify a VLAN; the range is 1 to 1001 and 1006 to 4094. |
|--------------------|------|----------------|---|
|--------------------|------|----------------|---|

Command Modes

User EXEC

Privileged EXEC

Command History

| Command History | Release | Modification |
|-----------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

Usage Guidelines

Use this command to display MLD snooping configuration for the switch or for a specific VLAN.

VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in MLD snooping.

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

Examples

This is an example of output from the show ipv6 mld snooping vlan command. It shows snooping characteristics for a specific VLAN.

```
Device# show ipv6 mld snooping vlan 100
Global MLD Snooping configuration:
-----
MLD snooping : Enabled
MLDv2 snooping (minimal) : Enabled
Listener message suppression : Enabled
TCN solicit query : Disabled
TCN flood query count : 2
Robustness variable : 3
Last listener query count : 2
Last listener query interval : 1000
Vlan 100:
-----
MLD snooping : Disabled
MLDv1 immediate leave : Disabled
Explicit host tracking : Enabled
Multicast router learning mode : pim-dvmrp
Robustness variable : 3
Last listener query count : 2
Last listener query interval : 1000
```

This is an example of output from the **show ipv6 mld snooping** command. It displays snooping characteristics for all VLANs on the switch.

```
Device# show ipv6 mld snooping
Global MLD Snooping configuration:
-----
MLD snooping : Enabled
MLDv2 snooping (minimal) : Enabled
Listener message suppression : Enabled
TCN solicit query : Disabled
TCN flood query count : 2
Robustness variable : 3
Last listener query count : 2
Last listener query interval : 1000

Vlan 1:
-----
MLD snooping : Disabled
MLDv1 immediate leave : Disabled
Explicit host tracking : Enabled
Multicast router learning mode : pim-dvmrp
Robustness variable : 1
Last listener query count : 2
Last listener query interval : 1000

<output truncated>

Vlan 951:
-----
MLD snooping : Disabled
MLDv1 immediate leave : Disabled
Explicit host tracking : Enabled
Multicast router learning mode : pim-dvmrp
Robustness variable : 3
Last listener query count : 2
Last listener query interval : 1000
```

show ipv6 mld snooping querier vlan

To see IPv6 MLD querier information in a VLAN, use the **show ipv6 mld snooping querier vlan** command.

```
show ipv6 mld snooping querier vlan vlan-id
```

| | |
|---------------------------|--|
| Syntax Description | <i>vlan-id</i> VLAN ID. Valid range is 1 to 1001 and 1006 to 4094. |
|---------------------------|--|

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

| | |
|----------------------|-----------------|
| Command Modes | Privileged EXEC |
|----------------------|-----------------|

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

Examples

The following example shows how to see the IPv6 MLD querier information in a VLAN whose ID is 3:

```
Device# show ipv6 mld snooping querier vlan 3
```

show ipv6 mld snooping wireless mgid

To see multicast group identifier (MGID) mapping information in the IPv6 MLD wireless related snooping events, use the **show ipv6 mld snooping wireless mgid** command.

```
show ipv6 mld snooping wireless mgid
```

Command Default None

Command Modes Privileged EXEC

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

Examples

The following example shows how to see multicast group identifier (MGID) mapping information in the IPv6 MLD wireless related snooping events:

```
Device# show ipv6 mld snooping wireless mgid
```

show ipv6 nd ra specific-route

To display information about IPv6 neighbor discovery router advertisement messages, use the **show ipv6 nd ra specific-route** command.

show ipv6 nd ra specific-route *interface*

| | |
|---------------------------|---|
| Syntax Description | <i>interface</i> Interface information. |
|---------------------------|---|

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

| | |
|----------------------|---------------------|
| Command Modes | Privileged EXEC (#) |
|----------------------|---------------------|

| Command History | Release | Modification |
|------------------------|-------------------------------|------------------------------|
| | Cisco IOS XE Bengaluru 17.6.1 | This command was introduced. |

| | |
|-------------------------|--|
| Usage Guidelines | If you do not specify the interface, routes configured under all the interfaces are displayed. |
|-------------------------|--|

| | |
|-----------------|---|
| Examples | The following example displays information about IPv6 neighbor discovery router advertisement messages: |
|-----------------|---|

```
Device# show ipv6 nd ra specific-route
```

show ldap attributes

To view information about the default LDAP attribute mapping, use the **show ldap attributes** command.

show ldap attributes

| | | |
|---------------------------|--------------------------------|------------------------------|
| Syntax Description | This command has no arguments. | |
| Command Default | None | |
| Command Modes | Global configuration | |
| Command History | Release | Modification |
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view information about the default LDAP attribute mapping:

```

Device# show ldap attributes
LDAP Attribute          Format      AAA Attribute
=====
airespaceBwDataBurstContract  Ulong     bsn-data-bandwidth-burst-contr
userPassword             String     password
airespaceBwRealBurstContract  Ulong     bsn-realtime-bandwidth-burst-c
employeeType             String     employee-type
airespaceServiceType      Ulong     service-type
airespaceACLName          String     bsn-acl-name
priv-lvl                  Ulong     priv-lvl
memberOf                  String DN  supplicant-group
cn                        String     username
airespaceDSCP              Ulong     bsn-dscp
policyTag                  String     tag-name
airespaceQOSLevel          Ulong     bsn-qos-level
airespace8021PType         Ulong     bsn-8021p-type
airespaceBwRealAveContract  Ulong     bsn-realtime-bandwidth-average
airespaceVlanInterfaceName  String     bsn-vlan-interface-name
airespaceVapId             Ulong     bsn-wlan-id
airespaceBwDataAveContract  Ulong     bsn-data-bandwidth-average-con
sAMAccountName            String     sam-account-name
meetingContactInfo         String     contact-info
telephoneNumber            String     telephone-number
Map: att_map_1
department                 String DN  element-req-qos

```

show ldap server

To view the LDAP server information, use the **show ldap server** command.

show ldap server { *server-name* | **all** }

| Syntax Description | |
|--------------------|---------------------------------|
| <i>server-name</i> | Name of the server. |
| all | Information of all the servers. |

Command Default None

Command Modes Privileged EXEC(#)

| Command History | Release | Modification |
|-----------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the LDAP server information:

```
Device# show ldap server all
```


show license air entities

To display information about active APs, new APs, and deleted APs in connection with a Cisco Catalyst Wireless Controller, enter the **show license air entities** command in privileged EXEC mode.

show license air entities { **added** | **bulk** | **deleted** | **no-change** | **summary** }

| Syntax Description | | |
|--------------------|--|--|
| added | Displays the list of newly reported APs. A newly added AP is one that was not listed in the last RUM report that the product instance generated. | |
| bulk | Displays the list of all currently active APs for the product instance | |
| deleted | Displays the list of deleted APs. A delete AP is one that was listed as active APs in the last RUM report that the product instance generated but is now disconnected. | |
| no-change | Displays the list of APs where there has been no change in the status since the last report. | |
| summary | Displays the RUM report generation particulars and information about active APs, new APs, and deleted APs, and indicates by when an acknowledgement (ACK) must be installed on the product instance. | |

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 | Command output was updated to display information relating to Smart Licensing Using Policy. |
| | Cisco IOS XE Cupertino 17.7.1 | The output of the show license air entities summary command was enhanced to display the following new field only on a Cisco Catalyst 9800-CL Wireless Controller: <code>License Ack expected within</code> |

Usage Guidelines **Smart Licensing:** If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing.

Smart Licensing Using Policy: If the software version on the device is Cisco IOS XE Amsterdam 17.3.2 or a later release, command output displays fields pertinent to Smart Licensing Using Policy.

Examples

For information about fields shown in the display for the **show license air entities summary** command, see [Table 5: show license air entities summary Field Descriptions, on page 234](#).

For sample output, see

- [show license air entities summary on a Cisco Catalyst 9800-CL Wireless Controller, on page 234](#)
- [show license air entities summary on a Cisco Catalyst 9800-L Wireless Controller, on page 235](#)

Table 5: show license air entities summary Field Descriptions

| Field | Description |
|---|--|
| Last license report time | When the last RUM report was generated, in the local time zone. |
| Upcoming license report time | When the next RUM report will be generated, in the local time zone. |
| No. of APs active at last report | Total number of APs listed as active APs in the last RUM report that was generated. |
| No. of APs newly added with last report | Number of new APs in the last RUM report that was generated. For example, if the number displayed here is 2, this means the <i>last but one</i> RUM report did not list these 2 APs, and are therefore newly added in the last RUM report that the product instance generated. |
| No. of APs deleted with last report | Total number of APs deleted as of the last RUM report that was generated. For example, if the number displayed here is 2, this means 2 APs were in the <i>last but one</i> RUM report, but were deleted in the <i>last</i> RUM report that was generated. |
| License Ack expected within | Note This field is displayed only on a Cisco Catalyst 9800-CL Wireless Controller running Cisco IOS XE Cupertino 17.7.1 or a later release. If the field is displayed, it means you must complete RUM reporting and ensure that the ACK is made available on the product instance - at least once. |

show license air entities summary on a Cisco Catalyst 9800-CL Wireless Controller

This example shows how to identify when an ACK is required on a Cisco Catalyst 9800-CL Wireless Controller

Beginning with Cisco IOS XE Cupertino 17.7.1, if you are using a Cisco Catalyst 9800-CL Wireless Controller, you must complete RUM reporting and ensure that the ACK is made available on the product instance - at least once. This is to ensure that correct and up-to-date usage information is reflected in CSSM.

Prior to 17.7.1, reporting and ACK installation was not *mandatory* for a Cisco Catalyst 9800-CL Wireless Controller.

The following is sample output on a Cisco Catalyst 9800-CL Wireless Controller, where an ACK must be made available on the product instance within 179 days. If this deadline is not met, currently active APs are not disconnected, but no new AP joins are allowed after the ACK deadline is passed. System messages are also displayed daily, until the first ACK is installed.

```
Device# show license air entities summary
Upcoming license report time.....: 21:05:16.092 UTC Mon Oct 25 2021
No. of APs active at last report.....: 57
No. of APs newly added with last report.....: 57
No. of APs deleted with last report.....: 0
License Ack expected within.....: 179 days
```

Detailed information about this requirement is available in the configuration guide. In the Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, version Cisco IOS XE Cupertino 17.7.1 onwards, see the *System Configuration* → *Smart Licensing Using Policy* → *RUM Reporting and Acknowledgment Requirement for Cisco Catalyst 9800-CL Wireless Controller*.

show license air entities summary on a Cisco Catalyst 9800-L Wireless Controller

The following is sample output on a Cisco Catalyst 9800-L Wireless Controller. Note how the output on this device does not display the `License Ack expected within` field. Reporting requirements on all Cisco Catalyst Wireless Controllers (except Cisco Catalyst 9800-CL Wireless Controller) are as per the standard guidelines in the Smart Licensing Using Policy environment: Reporting is required if the policy (**show license status**) or system messages indicate that it is.

```
Device# show license air entities summary
Upcoming license report time.....: 15:13:27.403 IST Tue Oct 26 2021
No. of APs active at last report.....: 1
No. of APs newly added with last report.....: 1
No. of APs deleted with last report.....: 0
```

show license all

To display all licensing information enter the **show license all** command in Privileged EXEC mode. This command displays status, authorization, UDI, and usage information, all combined.

show license all

Syntax Description

This command has no keywords or arguments

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 | Command output was updated to display information relating to Smart Licensing Using Policy. Command output no longer displays Smart Account and Virtual account information. |
| Cisco IOS XE Cupertino 17.7.1 | The output of the command was enhanced to display the following information: <ul style="list-style-type: none"> • RUM report statistics, in section <code>Usage Report Summary</code>. • Smart Account and Virtual Account information, in section <code>Account Information</code>. |

Usage Guidelines

Smart Licensing: If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing.

Smart Licensing Using Policy: If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2 or a later release, command output displays fields pertinent to Smart Licensing Using Policy.

This command concatenates the output of other **show license** commands, enabling you to display different kinds of licensing information together. For field descriptions, refer to the corresponding commands in the links provided below.

The `Smart Licensing Status` and `Account Information` sections of the **show license all** command corresponds with the output of the [show license status, on page 257](#) command.

The `License Usage` section of the **show license all** command corresponds with the output of the [show license usage, on page 286](#) command.

The `Product Information` section of the **show license all** command corresponds with the output of the [show license udi, on page 285](#) command.

The `Agent Version` section of the **show license all** command displays the Smart Agent version and is available only in this command.

The `License Authorizations` section of the **show license all** command corresponds with the output of the [show license authorization, on page 242](#) command.

The `Usage Report Summary` section of the **show license all** command corresponds with the output in the [show license tech, on page 270](#) command.

Examples

For sample output, see:

[Example: show license all \(Cisco Catalyst 9800-CL Wireless Controllers, 17.7.1\), on page 237](#)

[Example: show license all \(Cisco Catalyst 9800-CL Wireless Controllers\), on page 238](#)

Example: show license all (Cisco Catalyst 9800-CL Wireless Controllers, 17.7.1)

The following is sample output of the **show license all** command, on a product instance where the software version is Cisco IOS XE Cupertino 17.7.1. Note the addition of the two new sections in this release: `Account Information` and `Usage Report Summary`:

```
Device# show license all

Smart Licensing Status
=====

Smart Licensing is ENABLED

Export Authorization Key:
  Features Authorized:
    <none>

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Account Information:
  Smart Account: Eg-SA
  Virtual Account: Eg-VA

Data Privacy:
  Sending Hostname: yes
  Callhome hostname privacy: DISABLED
  Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license
  Proxy:
    Not Configured
  VRF:
    Not Configured

Miscellaneous:
  Custom Id: <empty>

Policy:
  Policy in use: Merged from multiple sources.
  Reporting ACK required: yes (CISCO default)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 365 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 90 (CISCO default)
```

```

Unenforced/Non-Export Subscription Attributes:
  First report requirement (days): 90 (CISCO default)
  Reporting frequency (days): 90 (CISCO default)
  Report on change (days): 90 (CISCO default)
Enforced (Perpetual/Subscription) License Attributes:
  First report requirement (days): 0 (CISCO default)
  Reporting frequency (days): 0 (CISCO default)
  Report on change (days): 0 (CISCO default)
Export (Perpetual/Subscription) License Attributes:
  First report requirement (days): 0 (CISCO default)
  Reporting frequency (days): 0 (CISCO default)
  Report on change (days): 0 (CISCO default)

Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: <none>
  Reporting push interval: 0 (no reporting)
  Next ACK push check: <none>
  Next report push: <none>
  Last report push: <none>
  Last report file write: <none>

Trust Code Installed: <none>

License Usage
=====

No licenses in use

Product Information
=====
UDI: PID:C9800-CL-K9,SN:9KGIXIDOXFE

HA UDI List:
  Active:PID:C9800-CL-K9,SN:9KGIXIDOXFE
  Standby:PID:C9800-CL-K9,SN:9UBKZU955E4

Agent Version
=====
Smart Agent for Licensing: 5.3.14_rel/47

License Authorizations
=====
Overall status:
  Active: PID:C9800-CL-K9,SN:9KGIXIDOXFE
    Status: NOT INSTALLED
  Standby: PID:C9800-CL-K9,SN:9UBKZU955E4
    Status: NOT INSTALLED

Purchased Licenses:
  No Purchase Information Available

Usage Report Summary:
=====
Total: 0, Purged: 0
Total Acknowledged Received: 0, Waiting for Ack: 0
Available to Report: 0 Collecting Data: 0

```

Example: show license all (Cisco Catalyst 9800-CL Wireless Controllers)

The following is sample output of the **show license all** command on a Cisco Catalyst 9800-CL Wireless Controller. Similar output is displayed on all supported Cisco Catalyst Wireless Controllers.

```
Device# show license all

Smart Licensing Status
=====

Smart Licensing is ENABLED
License Reservation is ENABLED

Export Authorization Key:
  Features Authorized:
    <none>

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Data Privacy:
  Sending Hostname: yes
  Callhome hostname privacy: DISABLED
  Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Transport Off

Miscellaneous:
  Custom Id: <empty>

Policy:
  Policy in use: Merged from multiple sources.
  Reporting ACK required: yes (CISCO default)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 365 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 90 (CISCO default)
    Reporting frequency (days): 90 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)

Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: <none>
  Reporting push interval: 0 (no reporting)
  Next ACK push check: Nov 01 20:31:46 2020 IST
  Next report push: <none>
  Last report push: <none>
  Last report file write: <none>

Trust Code Installed: <none>

License Usage
=====
```

```

air-network-advantage (DNA_NWStack):
  Description: air-network-advantage
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: air-network-advantage
  Feature Description: air-network-advantage
  Enforcement type: NOT ENFORCED
  License type: Perpetual
  Reservation:
    Reservation status: SPECIFIC INSTALLED
    Total reserved count: 20

air-dna-advantage (AIR-DNA-A):
  Description: air-dna-advantage
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: air-dna-advantage
  Feature Description: air-dna-advantage
  Enforcement type: NOT ENFORCED
  License type: Perpetual
  Reservation:
    Reservation status: SPECIFIC INSTALLED
    Total reserved count: 20

Product Information
=====
UDI: PID:C9800-CL-K9,SN:93BBAH93MGS

HA UDI List:
  Active:PID:C9800-CL-K9,SN:93BBAH93MGS
  Standby:PID:C9800-CL-K9,SN:9XECPSUU4XN

Agent Version
=====
Smart Agent for Licensing: 5.0.6_rel/47

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

Specified license reservations:
Aironet DNA Advantage Term Licenses (AIR-DNA-A):
  Description: DNA Advantage for Wireless
  Total reserved count: 20
  Enforcement type: NOT ENFORCED
  Term information:
    Active: PID:C9800-CL-K9,SN:93BBAH93MGS
      Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
      License type: TERM
      Start Date: 2020-OCT-14 UTC
      End Date: 2021-APR-12 UTC
      Term Count: 5
      Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
      License type: TERM

```



```
      Start Date: 2020-JUN-18 UTC
      End Date: 2020-DEC-15 UTC
      Term Count: 5
Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
  Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
  License type: TERM
    Start Date: 2020-OCT-14 UTC
    End Date: 2021-APR-12 UTC
    Term Count: 10
AP Perpetual Networkstack Advantage (DNA_NWStack):
  Description: AP Perpetual Network Stack entitled with DNA-A
  Total reserved count: 20
  Enforcement type: NOT ENFORCED
  Term information:
    Active: PID:C9800-CL-K9,SN:93BBAH93MGS
      Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
      License type: TERM
        Start Date: 2020-OCT-14 UTC
        End Date: 2021-APR-12 UTC
        Term Count: 5
      Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
      License type: TERM
        Start Date: 2020-JUN-18 UTC
        End Date: 2020-DEC-15 UTC
        Term Count: 5
    Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
      Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
      License type: TERM
        Start Date: 2020-OCT-14 UTC
        End Date: 2021-APR-12 UTC
        Term Count: 10

Purchased Licenses:
  No Purchase Information Available
```

show license authorization

To display authorization-related information for (export-controlled and enforced) licenses, enter the **show license authorization** command in privileged EXEC mode.

show license authorization

| | |
|---------------------------|---|
| Syntax Description | This command has no keywords or arguments |
|---------------------------|---|

| | |
|----------------------|-----------------|
| Command Modes | Privileged EXEC |
|----------------------|-----------------|

| | | |
|------------------------|--------------------------------|------------------------------|
| Command History | Release | Modification |
| | Cisco IOS XE Amsterdam 17.3.2a | This command was introduced. |

| | |
|-------------------------|--|
| Usage Guidelines | Only export-controlled or enforced licenses require authorization before use. While there are no export-controlled or enforced licenses on Cisco Catalyst Wireless Controllers, you can use this command to display migrated SLR authorization codes. |
|-------------------------|--|

Examples

See [Table 6: show license authorization Field Descriptions, on page 243](#) for information about fields shown in the display.

See [show license authorization Displaying Migrated Authorization Code, on page 245](#) for sample output.

Table 6: show license authorization Field Descriptions

| Field | Description |
|---------------------|--|
| Overall Status | <p>Header for UDI information for all product instances in the set-up, the type of authorization that is installed, and configuration errors, if any.</p> <p>In a High Availability set-up, all UDIs in the set-up are listed.</p> |
| Active: Status: | <p>The active product instance UDI, followed by the status of the authorization code installation for this UDI.</p> <p>If the status indicates that the authorization code is installed and there is a confirmation code, this is also displayed.</p> |
| Standby: Status: | <p>The standby product instance UDI, followed by the status of the authorization code installation for this UDI.</p> <p>If the status indicates that the authorization code is installed and there is a confirmation code, this is also displayed.</p> |
| Member: Status: | <p>The member product instance UDI, followed by the status of the authorization code installation for this UDI.</p> <p>If the status indicates that the authorization code is installed and there is a confirmation code, this is also displayed.</p> |
| ERROR: | <p>Configuration errors or discrepancies in the High Availability set-up, if any.</p> |

| Field | Description |
|------------------------|---|
| Authorizations | <p>Header for detailed license authorization information. All licenses, their enforcement types, and validity durations are displayed. Errors are displayed for each product instance if its authorization or mode does not match what is installed on the active.</p> <p>This section is displayed only if the product instance is using a license with an authorization code.</p> |
| () | License name and a shortened form of the license name. |
| Description | License description. |
| Total available count: | <p>Total count of licenses that are available to consume.</p> <p>This includes licenses of all durations (perpetual and subscription), including expired subscription licenses, for all the product instances in a High Availability setup.</p> |
| Enforcement type | <p>Enforcement type for the license. This may be one of the following:</p> <ul style="list-style-type: none"> • Enforced • Not enforced • Export-Controlled |
| Term information: | |

| Field | | Description |
|--------------------|--|---|
| | | <p>Header providing license duration information. The following fields maybe included under this header:</p> <ul style="list-style-type: none"> • Active: The active product instance UDI, followed by the status of the authorization code installation for this UDI. • Authorization type: Type of authorization code installed and date of installation. The type can be: SLAC, UNIVERSAL, SPECIFIED, PAK, RTU. • Start Date: Displays validity start date if the license is for a specific term or time period. • Start Date: Displays validity end date if the license is for a specific term or time period. • Term Count: License count. • Subscription ID: Displays ID if the license is for a specific term or time period. • License type: License duration. This can be: SUBSCRIPTION or PERPETUAL. • Standby: The standby product instance UDI, followed by the status of the authorization code installation for this UDI. • Member: The member product instance UDI, followed by the status of the authorization code installation for this UDI. <p>For more information about the duration or term of a license's validity, see <link tbd>.</p> |
| Purchased Licenses | Header for license purchase information. | |
| | Active: | The active product instance and its the UDI. |
| | Count: | License count. |
| | Description: | License description. |
| | License type: | License duration. This can be: SUBSCRIPTION or PERPETUAL. |
| | Standby: | The standby product instance UDI. |
| | Member: | The member product instance UDI. |

show license authorization Displaying Migrated Authorization Code

The following is sample output of the **show license authorization** command on a Cisco Catalyst 9800-CL Wireless Controller. The `Last Confirmation code:` shows that SLR authorization code is available after migration. Similar output is displayed on all supported Cisco Catalyst Wireless Controllers.

```

Device# show license authorization
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

Specified license reservations:
  Aironet DNA Advantage Term Licenses (AIR-DNA-A):
    Description: DNA Advantage for Wireless
    Total reserved count: 20
    Enforcement type: NOT ENFORCED
    Term information:
      Active: PID:C9800-CL-K9,SN:93BBAH93MGS
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
        Start Date: 2020-OCT-14 UTC
        End Date: 2021-APR-12 UTC
        Term Count: 5
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
        Start Date: 2020-JUN-18 UTC
        End Date: 2020-DEC-15 UTC
        Term Count: 5
      Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
        Start Date: 2020-OCT-14 UTC
        End Date: 2021-APR-12 UTC
        Term Count: 10
  AP Perpetual Networkstack Advantage (DNA_NWStack):
    Description: AP Perpetual Network Stack entitled with DNA-A
    Total reserved count: 20
    Enforcement type: NOT ENFORCED
    Term information:
      Active: PID:C9800-CL-K9,SN:93BBAH93MGS
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
        Start Date: 2020-OCT-14 UTC
        End Date: 2021-APR-12 UTC
        Term Count: 5
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
        Start Date: 2020-JUN-18 UTC
        End Date: 2020-DEC-15 UTC
        Term Count: 5
      Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
        Start Date: 2020-OCT-14 UTC
        End Date: 2021-APR-12 UTC
        Term Count: 10

Purchased Licenses:
  No Purchase Information Available

```

show license data conversion

To display license data conversion information, enter the **show license data** command in privileged EXEC mode.

show license data conversion

Syntax Description

This command has no keywords or arguments

Command Modes

Privileged EXEC (Device#)

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 with the introduction of Smart Licensing Using Policy. |

Usage Guidelines

Although visible on the CLI, this command is not applicable to Cisco Catalyst Wireless Controllers.

show license eventlog

To display event logs relating to Smart Licensing Using Policy, enter the **show license eventlog** command in privileged EXEC mode.

show license eventlog [*days*]

| Syntax Description | <i>days</i> Enter the number of days for which you want to display event logs. The valid value range is from 0 to 2147483647. | | | | | | |
|--------------------------------|---|---------|--------------|--------------------------------|------------------------------|--------------------------------|---|
| Command Modes | Privileged EXEC | | | | | | |
| Command History | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.10.1</td> <td>This command was introduced.</td> </tr> <tr> <td>Cisco IOS XE Amsterdam 17.3.2a</td> <td>Additional events were added with the introduction of Smart Licensing Using Policy: <ul style="list-style-type: none"> • Installation and removal of a policy • Request, installation and removal of an authorization code. • Installation and removal of a trust code. • Addition of authorization source information for license usage. </td> </tr> </tbody> </table> | Release | Modification | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. | Cisco IOS XE Amsterdam 17.3.2a | Additional events were added with the introduction of Smart Licensing Using Policy: <ul style="list-style-type: none"> • Installation and removal of a policy • Request, installation and removal of an authorization code. • Installation and removal of a trust code. • Addition of authorization source information for license usage. |
| Release | Modification | | | | | | |
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. | | | | | | |
| Cisco IOS XE Amsterdam 17.3.2a | Additional events were added with the introduction of Smart Licensing Using Policy: <ul style="list-style-type: none"> • Installation and removal of a policy • Request, installation and removal of an authorization code. • Installation and removal of a trust code. • Addition of authorization source information for license usage. | | | | | | |
| Usage Guidelines | <p>Smart Licensing Using Policy: If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2a or a later release, command output displays fields pertinent to Smart Licensing Using Policy.</p> <p>Smart Licensing: If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing.</p> | | | | | | |

show license history message

To display communication history between the product instance and CSSM or CSLU (as the case may be), enter the **show license history message** command in privileged EXEC mode. The output of this command is used by the technical support team, for troubleshooting.

show license history message

Syntax Description

This command has no keywords or arguments.

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|--------------------------------|------------------------------|
| Cisco IOS XE Amsterdam 17.3.2a | This command was introduced. |

Usage Guidelines

When you encounter an error message that you are not able to resolve, along with a copy of the message that appears on the console or in the system log, provide your Cisco technical support representative with sample output of these commands: **show license tech support**, **show license history message**, and the **show platform software sl-infra** privileged EXEC commands.

show license reservation

To display license reservation information, enter the **show license reservation** command in privileged EXEC mode.

show license reservation

| | |
|---------------------------|---|
| Syntax Description | This command has no keywords or arguments |
|---------------------------|---|

| | |
|----------------------|-----------------|
| 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 | This command continues to be available with the introduction of Smart Licensing Using Policy. |

| | |
|-------------------------|---|
| Usage Guidelines | The command continues to be available on the CLI and corresponding output is displayed, but with the introduction of Smart Licensing Using Policy, the notion of reservation is not longer applicable. Use the show license all command in privileged EXEC mode, to display <i>migrated</i> SLR licenses instead (the SLR authorization code is migrated to Smart Licensing Using Policy). |
|-------------------------|---|

show license rum

To display information about Resource Utilization Measurement reports (RUM report) available on the product instance, including report IDs, the current processing state of a report, error information (if any), and to save the detailed or summarized view that is displayed, enter the **show license rum** command in privileged EXEC mode.

```
show license rum { feature { license_name | all } | id { rum_id | all } } [ detail ] [ save path ]
```

| Syntax Description | | |
|---|--|---|
| feature { <i>license_name</i> all } | | Displays RUM report information based on the license name. Specify a particular license name to display all RUM reports for that license, or use the all keyword to display all RUM reports available on the product instance. |
| id { <i>rum_id</i> all } | | Displays RUM report information based on the RUM report ID. Specify a report ID to display information for a single report, or use the all keyword to display all RUM reports available on the product instance. |
| detail | | Displays detailed RUM report information. You can use this to display detailed information by license name and detailed information by RUM report ID. |
| save path | | Saves the information that is displayed. This can be the simplified or detailed version and depends on the preceding keywords you have entered. Information about 200 RUM reports can be displayed. If there are more 200 RUM reports on the product instance, you can view information about all the RUM reports by saving it to a text (.txt) file. Note This option saves the information <i>about</i> RUM reports and is not for reporting purposes. It does not save the RUM report, which is an XML file containing usage information. |

Command Modes Privileged EXEC (Device#)

| Command History | Release | Modification |
|-----------------|-------------------------------|------------------------------|
| | Cisco IOS XE Cupertino 17.7.1 | This command was introduced. |

Usage Guidelines A RUM report is a license usage report, which the product instance generates, to fulfil reporting requirements as specified by the policy. An acknowledgement (ACK) is a response from CSSM and provides information about the status of a RUM report. Once the ACK for a report is available on the product instance, it indicates

that the corresponding RUM report is no longer required and can be deleted. You can use the **show license rum** command to:

- Display information about the available RUM reports on the product instance - filtered by ID or license name.
- Display a short summary of the information or display a detailed view of the information.
- Track a RUM report throughout its lifecycle (from the time it is first generated until its acknowledgement from CSSM). By displaying the current processing state and condition of a report you can ascertain if and when there is a problem in the reporting workflow.
- Save the displayed information. The CLI displays information about up to 200 reports. If there are more than 200 reports on the product instance and you want to view information about all of them, save the displayed info in a .txt file and export to the desired location to view.

To display a statistical view of RUM report information (the total number of reports on the product instance, the number of reports that have a corresponding ACK, the number of reports waiting for an ACK etc.) refer to the `Usage Report Summary`: section of the **show license all** and **show license tech** privileged EXEC commands.

The **show license tech** command also provides RUM report related information that the Cisco technical support team can use to troubleshoot, if there are problems with RUM reporting.

Examples

For information about fields shown in the display, see [#unique_1059 unique_1059_Connect_42_table_ytd_q4m_hrb](#) and [#unique_1059 unique_1059_Connect_42_table_gtn_q4m_hrb](#)

For sample output of the **show license rum** command, see:

- [#unique_1059 unique_1059_Connect_42_example_ugm_lsd_4rb](#)
- [#unique_1059 unique_1059_Connect_42_example_stg_msd_4rb](#)

Table 7: show license rum (simplified view) Field Descriptions

| Field Name | Description |
|------------|---|
| Report Id | A numeric field that identifies a RUM report. The product instance automatically assigns an ID to every RUM report it generates. An ID may be up to 20 characters long. |

| Field Name | Description |
|--------------|---|
| State | <p>This field displays the current processing state of a RUM report, and can be only one of the following:</p> <ul style="list-style-type: none"> • OPEN: This means new measurements are been added into this report. • CLOSED: This means no new measurements can be added to this report, and the report is ready for communication to CSSM. • PENDING: This is a transitional status that you may see if you display a report while it is being transmitted. • UNACK: This means the report was transmitted and is waiting for confirmation from CSSM, that it is processed. • ACK: This means the report was processed or acknowledged by CSSM and is eligible for deletion. |
| Flag | <p>Indicates the condition of the RUM report, and is displayed in the form of a character. Each character represents a specific condition, and can be only one of the following values:</p> <ul style="list-style-type: none"> • N: Normal; This means no errors have been detected and the report is going through normal operation. • P: Purged; This means the report was removed due to system resource limitation, and can refer to a shortage of disk space or insufficient memory. If this flag is displayed, refer to the <code>State Change Reason</code> field in the detailed view for more information. • E: Error; This means an error was detected in the RUM report. If this flag is displayed, refer to the detailed view for more information. Possible workflow issues include and are not limited to the following: <ul style="list-style-type: none"> • RUM report was dropped by CSSM. If this is the issue, the <code>State</code> field displays value <code>ACK</code>, but the <code>State Change Reason</code> does not change to <code>ACKED</code>. • RUM Report data is missing. If this is the issue, the <code>Storage State</code> field displays value <code>MISSING</code>. • Tracking information is missing. If this is the case the <code>State</code> field displays value <code>UNACK</code> and the <code>Transaction ID</code> field has no information. <p>Note Occasional errors in RUM reports do not require any action from you and are not an indication of a problem. It is only if you see a large number of reports (greater than 10) with errors that you must contact the Cisco technical support team.</p> |
| Feature Name | The name of the license that the RUM report applies to. |

Table 8: show license rum (detailed view) Field Descriptions

| Field Name | Description |
|----------------------|---|
| Report Id | A numeric field that identifies a RUM report. The product instance automatically assigns an ID to every RUM report it generates. An ID may be up to 20 characters long. |
| Metric Name: | Shows the type of data that is recorded. For a RUM report, the only possible value is ENTITLEMENT, and refers to measurement of license usage. |
| Feature Name: | The name of the license that the RUM report applies to. |
| Metric Value | A unique identifier for the data that is recorded. This is the same as the “Entitlement Tag” in the output of the show license tech command and it displays information about the license being tracked. |
| UDI | Composed of the Product ID (PID) and serial number of the product instance. |
| Previous Report Id: | ID of the previous RUM report that the product instance generated for a license. |
| Next Report Id: | The ID that the product instance will use for the next RUM report it generates for a license. |
| State: | Displays the current processing state of a RUM report. The value displayed here is always the same as the value displayed in the simplified view. For the list of possible values see #unique_1059 unique_1059_Connect_42_table_ytd_q4m_hrb above. |
| State Change Reason: | Displays the reason for a RUM report state change. Not all state changes provide a reason. <ul style="list-style-type: none"> • NONE: This means the RUM report is going through its normal lifecycle (for instance, from OPEN → CLOSED → ACK). This state change reason is usually accompanied by an N flag (meaning Normal) in the simplified view and requires no action from you. • ACKED: RUM report was processed normally by CSSM. • REMOVED: RUM report was received and requested to be removed by CSSM. • RELOAD: RUM report state was changed due to some type of device reload. |
| Start Time: | Timestamps for measurement start and measurement end for a RUM report. |
| End Time: | Together, the start time and end time provide the time duration that the measurements cover. |

| Field Name | Description |
|----------------------|--|
| Storage State: | <p>Displays current storage state of the RUM report and can be one of the following values:</p> <ul style="list-style-type: none"> • EXIST: This means the data for the RUM report is located in storage. • DELETED: This means the data was intentionally deleted. Refer to the <code>Storage State Change Reason</code> in the output of the show license tech command for more information about this storage state. • PURGED: This means the data was deleted due to a system resource limitation. Refer to the <code>Storage State Change Reason</code> in the output of the show license tech command for more information about this storage state. • MISSING: This means data is missing from storage. If reports are identified as missing, there is no recovery process. |
| Transaction ID: | <p>Contains tracking information for the RUM report. This information can be either polling information or ACK import information.</p> <p>The Transaction Message contains the error message, if the product instance receives one when importing an ACK.</p> <p>The information in these fields is used by the Cisco technical support team when troubleshooting problems with RUM reports.</p> |
| Transaction Message: | |

Example: show license rum feature: Simplified and Detailed View

The following is sample output of the **show license rum feature***license-name* and **show license rum feature***license-name***detail** commands on a Cisco Catalyst 9500 Series Switch. Similar output is displayed on all other Catalyst switches.

The output is filtered to display all RUM reports for the DNA Advantage license, followed by a detailed view of all RUM reports for the DNA Advantage license.

```

Device# show license rum feature air-dna-advantage

Smart Licensing Usage Report:
=====
Report Id,           State,    Flag, Feature Name
1638055644          CLOSED   N      air-dna-advantage
1638055646          OPEN    N      air-dna-advantage

Device# show license rum feature air-dna-advantage detail
Smart Licensing Usage Report Detail:
=====
Report Id: 1638055644
Metric Name: ENTITLEMENT
Feature Name: air-dna-advantage
Metric Value: regid.2017-08.com.cisco.AIR-DNA-A,1.0_b6308627-3ab0-4a11-a3d9-586911a0d790
UDI: PID:C9800-CL-K9,SN:93SZ7RXN93Y
Previous Report Id: 0, Next Report Id: 1638055646
    
```

```
State: CLOSED,          State Change Reason: RELOAD
Start Time: Nov 28 12:02:09 2021 UTC,      End Time: Nov 30 22:02:13 2021 UTC
Storage State: EXIST
Transaction ID: 0
Transaction Message: <none>
```

```
Report Id: 1638055646
Metric Name: ENTITLEMENT
Feature Name: air-dna-advantage
Metric Value: regid.2017-08.com.cisco.AIR-DNA-A,1.0_b6308627-3ab0-4a11-a3d9-586911a0d790
UDI: PID:C9800-CL-K9,SN:93SZ7RXN93Y
Previous Report Id: 1638055644,      Next Report Id: 0
State: OPEN,           State Change Reason: None
Start Time: Nov 30 23:12:56 2021 UTC,      End Time: Dec 01 02:12:56 2021 UTC
Storage State: EXIST
Transaction ID: 0
Transaction Message: <none>
```

Example: Saving a RUM Report View

The following example shows you how to save the information that is displayed.

By using the **feature** and **all** keywords, the output is filtered to display all RUM reports for all licenses being used on the product instance. It is then transferred to a TFTP location, from where it can be opened, to view the information.

```
Device# show license rum feature all save bootflash:all-rum-stats.txt
Device# copy tftp://10.8.0.6/bootflash:all-rum-stats.txt
```


show license status

To display information about licensing settings such as data privacy, policy, transport, usage reporting and trust codes, enter the **show license status** command in privileged EXEC mode.

show license status

| | | |
|-------------------------------|--|--|
| Syntax Description | This command has no keywords or arguments | |
| Command Modes | Privileged EXEC (Device#) | |
| Command History | Release | Modification |
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |
| | Cisco IOS XE Amsterdam 17.3.2a | Command output was updated to reflect new fields that are applicable to Smart Licensing Using Policy. This includes <code>Trust code installed:</code> , <code>Policy in use</code> , <code>Policy name:</code> , reporting requirements as in the policy (<code>Attributes:</code>), and fields related to usage reporting. Command output no longer displays Smart Account and Virtual account information. |
| Cisco IOS XE Cupertino 17.7.1 | Command output was updated to display Smart Account and Virtual account information. | |

Usage Guidelines

Smart Licensing: If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing.

Smart Licensing Using Policy: If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2a or a later release, command output displays fields pertinent to Smart Licensing Using Policy.

Account Information in the output

Starting with Cisco IOS XE Cupertino 17.7.1, every ACK includes the Smart Account and Virtual Account that was reported to, in CSSM. When it receives the ACK, the product instance securely stores only the latest version of this information - as determined by the timestamp in the ACK. The Smart Account and Virtual Account information that is displayed in the `Account Information` section of this command's output is therefore always as per the latest available ACK on the product instance.

If a product instance is moved from one Smart Account and Virtual Account to another, the next ACK after the move will have this updated information. The output of this command is updated once this ACK is available on the product instance.

The ACK may be received directly (where the product instance is connected to CSSM), or indirectly (where the product instance is connect to CSSM through CSLU, Cisco DNA Center, or SSM On-Prem), or by manually importing the ACK (where a product instance is in an air-gapped network).

Examples

For information about the fields shown in the display, see [Table 9: show license status Field Descriptions for Smart Licensing Using Policy, on page 258](#).

For sample output, see:

- [show license status with Account Information \(Smart Licensing Using Policy\), on page 263](#)
- [show license status with Cisco Default Policy \(Smart Licensing Using Policy\), on page 264](#)
- [show license status with Custom Policy \(Smart Licensing Using Policy\), on page 265](#)

Table 9: show license status Field Descriptions for Smart Licensing Using Policy

| Field | Description | |
|-------------------------------|--|---|
| Utility | Header for utility settings that are configured on the product instance. | |
| | Status: | Status |
| | Utility report: | Last attempt: |
| | Customer Information: | The following fields are displayed: <ul style="list-style-type: none"> • Id: • Name: • Street • City: • State: • Country: • Postal Code: |
| Smart Licensing Using Policy: | Header for policy settings on the product instance. | |
| | Status: | Indicates if Smart Licensing Using Policy is enabled. Smart Licensing Using Policy is supported starting from Cisco IOS XE Amsterdam 17.3.2 and is always enabled on supported software images. |

| Field | Description | |
|----------------------|--|---|
| Account Information: | Header for account information that the product instance belongs to, in CSSM. This section is displayed only if the software version on the product instance is Cisco IOS XE Cupertino 17.7.1 or a later release. | |
| | Smart Account: | The Smart Account that the product instance is part of. This information is always as per the latest available ACK on the product instance. |
| | Virtual Account: | The Virtual Account that the product instance is part of. This information is always as per the latest available ACK on the product instance. |
| Data Privacy: | Header for privacy settings that are configured on the product instance. | |
| | Sending Hostname: | A <i>yes</i> or <i>no</i> value which shows if the hostname is sent in usage reports. |
| | Callhome hostname privacy: | Indicates if the Call Home feature is configured as the mode of transport for reporting. If configured, one of these values is displayed: <ul style="list-style-type: none"> • ENABLED • DISABLED |
| | Smart Licensing hostname privacy: | One of these values is displayed: <ul style="list-style-type: none"> • ENABLED • DISABLED |
| | Version privacy: | One of these values is displayed: <ul style="list-style-type: none"> • ENABLED • DISABLED |
| Transport: | Header for transport settings that are configured on the product instance. | |
| | Type: | Mode of transport that is in use. Additional fields are displayed for certain transport modes. For example, if transport type is set to CSLU, the CSLU address is also displayed. |

| Field | Description |
|--|---|
| Policy: | Header for policy information that is applicable to the product instance. |
| Policy in use: | Policy that is applied This can be one of the following: Cisco default, Product default, Permanent License Reservation, Specific License Reservation, PAK license, Installed on <date>, Controller. |
| Policy name: | Name of the policy |
| Reporting ACK required: | A <i>yes</i> or <i>no</i> value which specifies if the report for this product instance requires CSSM acknowledgement (ACK) or not. The default policy is always set to “yes”. |
| Unenforced/Non-Export Perpetual Attributes | Displays policy values for perpetual licenses. <ul style="list-style-type: none"> • First report requirement (days): The maximum amount of time available before the first report must be sent, followed by policy name. • Reporting frequency (days): The maximum amount of time available before the subsequent report must be sent, followed by policy name. • Report on change (days): he maximum amount of time available to send a report in case of a change in license usage, followed by policy name |
| Unenforced/Non-Export Subscription Attributes | Displays policy values for subscription licenses. <ul style="list-style-type: none"> • First report requirement (days): The maximum amount of time available before the first report must be sent, followed by policy name. • Reporting frequency (days): The maximum amount of time available before the subsequent report must be sent, followed by policy name. • Report on change (days): he maximum amount of time available to send a report in case of a change in license usage, followed by policy name |
| Enforced (Perpetual/Subscription) License Attributes | |

| Field | | Description |
|---------------|--|--|
| | | <p>Displays policy values for enforced licenses.</p> <ul style="list-style-type: none"> • First report requirement (days): The maximum amount of time available before the first report must be sent, followed by policy name. • Reporting frequency (days): The maximum amount of time available before the subsequent report must be sent, followed by policy name. • Report on change (days): The maximum amount of time available to send a report in case of a change in license usage, followed by policy name |
| | Export (Perpetual/Subscription) License Attributes | <p>Displays policy values for export-controlled licenses.</p> <ul style="list-style-type: none"> • First report requirement (days): The maximum amount of time available before the first report must be sent, followed by policy name. • Reporting frequency (days): The maximum amount of time available before the subsequent report must be sent, followed by policy name. • Report on change (days): The maximum amount of time available to send a report in case of a change in license usage, followed by policy name |
| Miscellaneous | Header for custom ID. | |
| | Custom Id: | ID |

| Field | Description |
|-------------------------|--|
| Usage Reporting: | Header for usage reporting (RUM reports) information. |
| Last ACK received: | Date and time of last ACK received, in the local time zone. |
| Next ACK deadline: | Date and time for next ACK. If the policy states that an ACK is not required then this field displays <code>none</code> . Note If an ACK is required and is not received by this deadline, a syslog is displayed. |
| Reporting Interval: | Reporting interval in days The value displayed here depends on what you configure in the license smart usage interval <code>interval_in_days</code> and the policy value. For more information, see the corresponding Syntax Description: license smart (global config) . |
| Next ACK push check: | Date and time when the product instance will submit the next polling request for an ACK. Date and time are in the local time zone. This applies only to product instance- initiated communication to CSSM or CSLU. If the reporting interval is zero, or if no ACK polling is pending, then this field displays <code>none</code> . |
| Next report push: | Date and time when the product instance will send the next RUM report. Date and time are in the local time zone. If the reporting interval is zero, or if there are no pending RUM reports, then this field displays <code>none</code> . |
| Last report push: | Date and time for when the product instance sent the last RUM report. Date and time are in the local time zone. |
| Last report file write: | Date and time for when the product instance last saved an offline RUM report. Date and time are in the local time zone. |
| Last report pull: | Date and time for when usage reporting information was retrieved using data models. Date and time are in the local time zone. |

| Field | Description |
|-----------------------|--|
| Trust Code Installed: | Header for trust code-related information. Displays date and time if trust code is installed. Date and time are in the local time zone. If a trust code is not installed, then this field displays <i>none</i> . |
| Active: | Active product instance. In a High Availability set-up, the the UDIs of all product instances in the set-up, along with corresponding trust code installation dates and times are displayed. |
| Standby: | Standby product instance. |
| Member: | Member product instance |

show license status with Account Information (Smart Licensing Using Policy)

The following is sample output of the **show license status** command, on a product instance where the software version is Cisco IOS XE Cupertino 17.7.1:

```

Device# show license status
Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Account Information:
  Smart Account: Eg-SA
  Virtual Account: Eg-VA

Data Privacy:
  Sending Hostname: yes
  Callhome hostname privacy: DISABLED
  Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license
  Proxy:
    Not Configured
  VRF:
    Not Configured

Policy:
  Policy in use: Merged from multiple sources.
  Reporting ACK required: yes (CISCO default)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 365 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 90 (CISCO default)
    Reporting frequency (days): 90 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Enforced (Perpetual/Subscription) License Attributes:
  
```

```

    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)
Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)

Miscellaneous:
    Custom Id: <empty>

Usage Reporting:
    Last ACK received: <none>
    Next ACK deadline: <none>
    Reporting push interval: 0 (no reporting)
    Next ACK push check: <none>
    Next report push: <none>
    Last report push: <none>
    Last report file write: <none>

Trust Code Installed: <none>

```

show license status with Cisco Default Policy (Smart Licensing Using Policy)

The following is sample output of the **show license status** command; a default is policy applied here.

```

Device# show license status

Utility:
    Status: DISABLED

Smart Licensing Using Policy:
    Status: ENABLED

Data Privacy:
    Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
    Version privacy: DISABLED

Transport:
    Type: Smart
    URL: https://smartreceiver.cisco.com/licservice/license
    Proxy:
    Not Configured

Policy:
    Policy in use: Merged from multiple sources.
    Reporting ACK required: yes (CISCO default)
    Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 365 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 90 (CISCO default)
    Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 90 (CISCO default)
    Reporting frequency (days): 90 (CISCO default)
    Report on change (days): 90 (CISCO default)
    Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)
    Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)

```



```
Report on change (days): 0 (CISCO default)

Miscellaneous:
  Custom Id: <empty>

Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: <none>
  Reporting push interval: 0 (no reporting)
  Next ACK push check: <none>
  Next report push: <none>
  Last report push: <none>
  Last report file write: <none>

Trust Code Installed: <none>
```

show license status with Custom Policy (Smart Licensing Using Policy)

The following is sample output of the **show license status** command; a custom policy applied here.

```
Device# show license status
Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Data Privacy:
  Sending Hostname: yes
  Callhome hostname privacy: DISABLED
  Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license
  Proxy:
    Not Configured

Policy:
  Policy in use: Installed On Nov 02 05:09:31 2020 IST
  Policy name: SLE Policy
  Reporting ACK required: yes (Customer Policy)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 60 (Customer Policy)
    Reporting frequency (days): 60 (Customer Policy)
    Report on change (days): 60 (Customer Policy)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 30 (Customer Policy)
    Reporting frequency (days): 30 (Customer Policy)
    Report on change (days): 30 (Customer Policy)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 90 (Customer Policy)
    Report on change (days): 90 (Customer Policy)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 90 (Customer Policy)
    Report on change (days): 90 (Customer Policy)

Miscellaneous:
  Custom Id: <empty>
```

```
Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: <none>
  Reporting push interval: 0 (no reporting)
  Next ACK push check: <none>
  Next report push: <none>
  Last report push: <none>
  Last report file write: <none>
```

```
Trust Code Installed:
  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
          INSTALLED on Nov 02 05:09:31 2020 IST
  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
           INSTALLED on Nov 02 05:09:31 2020 IST
```

show license summary

To display a brief summary of license usage, which includes information about licenses being used, the count, and status, enter the **show license summary** command in privileged EXEC mode.

show license summary

| | | |
|---------------------------|---|---|
| Syntax Description | This command has no keywords or arguments | |
| 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 | Command output was updated to reflect valid license status for Smart Licensing Using Policy. Valid license statuses include: <code>IN USE</code> , <code>NOT IN USE</code> , <code>NOT AUTHORIZED</code> . Command output was also updated to remove registration and authorization information. Command output no longer displays Smart Account and Virtual account information. |
| | Cisco IOS XE Cupertino 17.7.1 | Command output was updated to display Smart Account and Virtual account information. |

Usage Guidelines

Smart Licensing: If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing.

Smart Licensing Using Policy: If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2a or a later release, command output displays fields pertinent to Smart Licensing Using Policy.

The licenses on Cisco Catalyst Wireless Controllers are never `NOT AUTHORIZED`, because none of the available licenses are export-controlled or enforced (Only these licenses require authorization before use).

Account Information in the output

Starting with Cisco IOS XE Cupertino 17.7.1, every ACK includes the Smart Account and Virtual Account that was reported to, in CSSM. When it receives the ACK, the product instance securely stores only the latest version of this information - as determined by the timestamp in the ACK. The Smart Account and Virtual Account information that is displayed in the `Account Information` section of this command's output is therefore always as per the latest available ACK on the product instance.

If a product instance is moved from one Smart Account and Virtual Account to another, the next ACK after the move will have this updated information. The output of this command is updated once this ACK is available on the product instance.

The ACK may be received directly (where the product instance is connected to CSSM), or indirectly (where the product instance is connect to CSSM through CSLU, Cisco DNA Center, or SSM On-Prem), or by manually importing the ACK (where a product instance is in an air-gapped network).

Examples

See [Table 10: show license summary Field Descriptions, on page 268](#) for information about fields shown in the display.

[show license summary: IN USE \(Smart Licensing Using Policy\), on page 268](#)

[show license summary: NOT IN USE \(Smart Licensing Using Policy\), on page 268](#)

Table 10: show license summary Field Descriptions

| Field | Description |
|--|--|
| Account Information: Smart Account: Virtual Account: | The Smart Account and Virtual Account that the product instance is part of. This information is always as per the latest available ACK on the product instance. This field is displayed only if the software version on the product instance is Cisco IOS XE Cupertino 17.7.1 or a later release. |
| License | Name of the licenses in use |
| Entitlement Tag | Short name for license |
| Count | License count |
| Status | License status can be one of the following <ul style="list-style-type: none"> • In-Use: Valid license, and in-use. • Not In-Use • Not Authorized: Means that the license requires installation of SLAC before use. |

show license summary: IN USE (Smart Licensing Using Policy)

The following is sample output of the **show license summary** command, on a product instance where the software version is Cisco IOS XE Cupertino 17.7.1:

```
Device# show license summary
```

```
Account Information:
  Smart Account: Eg-SA
  Virtual Account: Eg-VA
```

```
License Usage:
License                Entitlement Tag                Count Status
-----
air-network-essentials (DNA_NWSTACK_E)                1 IN USE
air-dna-essentials     (AIR-DNA-E)                    1 IN USE
```

show license summary: NOT IN USE (Smart Licensing Using Policy)

The following is sample output of the **show license summary** command, where no APs have joined the controller. Current consumption (Count) is therefore zero, and the `Status` field shows that the licenses are NOT IN USE:

```
Device# show license summary
```

```
Device#show license summary  
License Reservation is ENABLED
```

```
License Usage:
```

| License | Entitlement Tag | Count | Status |
|-------------------------|-----------------|-------|------------|
| Aironet DNA Advantag... | (AIR-DNA-A) | 0 | NOT IN USE |
| AP Perpetual Network... | (DNA_NWStack) | 0 | NOT IN USE |

show license tech

To display licensing information to help the technical support team to solve a problem, enter the **show license tech** command in privileged EXEC mode. The output for this command includes outputs of several other **show license** commands and more.

```
show license tech { message | rum { feature { license_name | all } | id { rum_id | all } } [ detail ] [ save_path ] | support }
```

Syntax Description

| | |
|--|--|
| message | Displays messages concerning trust establishment, usage reporting, result polling, authorization code requests and returns, and trust synchronization. This is the same information as displayed in the output of the show license history message command. |
| rum { feature { license_name all } id { rum_id all } } [detail] [save_path] | Displays information about Resource Utilization Measurement reports (RUM reports) on the product instance, including report IDs, the current processing state of a report, error information (if any), and an option save the displayed RUM report information. Note This option saves the information <i>about</i> RUM reports and is not for reporting purposes. It does not save the RUM report, which is an XML file containing usage information. |
| support | Displays licensing information that helps the technical support team to debug a problem. |

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 | Command output was updated to reflect new fields that are applicable to Smart Licensing Using Policy. |

| Release | Modification |
|-------------------------------|--|
| Cisco IOS XE Cupertino 17.7.1 | <p>The rum keyword and additional options under this keyword were added:</p> <pre>{ feature { license_name all } id { rum_id all } }</pre> <p>The output of the show license tech support command was enhanced to display the following information:</p> <ul style="list-style-type: none"> • RUM report information, in section <code>License Usage and Usage Report Summary</code>. • Smart Account and Virtual account information, in section <code>Account Information</code>. <p>The data conversion, eventlog and reservation keywords were removed from this command. They continue to be available as separate show commands, that is, show license data, show license eventlog, and show license reservation respectively.</p> |

Usage Guidelines

Smart Licensing: If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing (whether smart licensing is enabled, all associated licensing certificates, compliance status, and so on).

Smart Licensing Using Policy: If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2 or a later release, command output displays fields pertinent to Smart Licensing Using Policy. Note the following guidelines:

- Troubleshooting with a Support Representative

When you encounter an error message that you are not able to resolve, along with a copy of the message that appears on the console or in the system log, provide your Cisco technical support representative with sample output of these commands: **show license tech support**, **show license history message**, and the **show platform software sl-infra all** privileged EXEC commands.

- RUM Report Information in the output

- The output of the **show license tech support** command displays the following sections pertaining to RUM reports:

[Table 11: show license tech support: Field Descriptions for Header "License Usage", on page 272](#)

```
<output truncated>
License Usage
=====
Measurements:
  ENTITLEMENT:
    Interval: 00:15:00
    Current Value: 800
    Current Report: 1638055645          Previous: 0
<output truncated>
```

[Table 12: show license tech support: Field Descriptions for Header "Usage Report Summary", on page 273](#)

```
<output truncated>
Usage Report Summary:
=====
Total: 4, Purged: 0 (0)
```

```
Total Acknowledged Received: 0, Waiting for Ack: 0(4)
Available to Report: 4 Collecting Data: 2
Maximum Display: 4 In Storage: 4, MIA: 0(0)
Report Module Status: Ready
```

<output truncated>

- The output of the **show license tech rum** command when used with the **detail** keyword, displays the following fields pertaining to RUM reports: [Table 13: show license tech rum: Field Descriptions for Header "Smart Licensing Usage Report Detail"](#), on page 273.

The options available under the **show license tech rum** keyword are the same as the options available with the **show license rum** privileged EXEC command. The sample output that is displayed in the *simplified view* is also the same. But if you use the **detail** keyword (for example if you enter **show license tech rum feature license_name detail**), the detailed view is displayed and this has a few *additional* fields when compared to **show license rum**.

```
<output truncated>
Smart Licensing Usage Report Detail:
=====
Report Id: 1638055644
  Metric Name: ENTITLEMENT
  Feature Name: air-dna-advantage
  Metric Value:
regid.2017-08.com.cisco.AIR-DNA-A,1.0_b6308627-3ab0-4a11-a3d9-586911a0d790
  UDI: PID:C9800-CL-K9,SN:93SZ7RXN93Y
  Previous Report Id: 0, Next Report Id: 1638055646
  Version: 2.0
  State: CLOSED, State Change Reason: RELOAD
  Start Time: Nov 28 12:02:09 2021 UTC, End Time: Nov 30 22:02:13 2021 UTC
  Storage State: EXIST, Storage State Change Reason: None
  Transaction ID: 0
  Transaction Message: <none>
  Report Size: 54880(54987)
<output truncated>
```

Table 11: show license tech support: Field Descriptions for Header "License Usage"

| Field Name | Description |
|-----------------|---|
| Interval: | This is a fixed measurement duration and is always 15 minutes. |
| Current Value: | Information about the current license count. |
| Current Report: | ID of the currently OPEN report for the license. |
| Previous: | ID of the last OPEN report for the license. This report will have state CLOSED now. |

Table 12: show license tech support: Field Descriptions for Header "Usage Report Summary"

| Field Name | Description |
|------------------------------|--|
| Total: | Total number of reports that the product instance has ever generated. Note This total does not refer to the total number of reports <i>currently available</i> on and being tracked by the product instance. For this you must sum up the <code>Total Acknowledged Received:</code> and <code>Available to Report</code> fields. |
| Purged: | The number of reports deleted due to a system resource limitation. This number includes RUM reports where the product instance no longer has tracking information. |
| Total Acknowledged Received: | The number of RUM reports acknowledged on this product instance. |
| Waiting for Ack: | The number of RUM reports waiting for an ACK. This is the total number of reports in an <code>UNACK</code> state, where the product instance still has tracking information. |
| Available to Report: | The number of RUM reports that are available to send to CSSM. This is the total number of reports in an <code>OPEN</code> or <code>CLOSED</code> state, where the product instance still has tracking information. |
| Collecting Data: | Number of reports where the product instance is currently collecting measurements. |
| Maximum Display: | Number of reports available for display in a show command's output. |
| In Storage: | Number of reports currently stored on the disk |
| MIA: | The number of reports missing. |

Table 13: show license tech rum: Field Descriptions for Header "Smart Licensing Usage Report Detail"

| Field Name | Description |
|------------|---|
| Version: | Displays the format of the report during transmission. Starting with Cisco IOS XE Cupertino 17.7.1, RUM reports are stored in a new format that reduces processing time. This field indicates if the product instance is using the old format or the new format. |

| Field Name | Description |
|---|---|
| Storage State: | <p>Indicates if a given report is currently in storage.</p> <p>In addition to the displaying the current storage state of the RUM report, with these possible values: EXIST, DELETED, PURGED, MISSING, if a "(1)" is displayed next to the label (<code>Storage State (1)</code>), this means the RUM report is in the older (pre-17.7.1 format) and will be processed accordingly. If the RUM report is in the new format, the field is displayed as <code>Storage State</code> - without any extra information.</p> |
| Storage State Change Reason: | <p>Displays the reason for the change in the storage state change. Not all state changes provide a reason.</p> <ul style="list-style-type: none"> • NONE: This means no reason was recorded for the the storage state change. • PROCESSED: This means the RUM report was deleted after CISCO has processed the data. • LIMIT_STORAGE: This means the RUM report was deleted because the product instance reached it's storage limit. • LIMIT_TIME: This means the RUM report was deleted because the report reached the persisted time limit. |
| Transaction ID: Transaction Message: | <p>If the transaction ID displays a correlation ID and an error status is displayed, the product instance displays the error code field in this section. If there are no errors, no data is displayed here.</p> |
| Report Size | <p>This field displays two numbers. The first number is the size of raw report for communication, in bytes. The second number is the disk space used for saving the report, also in bytes. The second number is displayed only if report is stored in the new format.</p> |

show license tech support on Cisco Catalyst 9800-CL Wireless Controller

The following is sample output from the **show license tech support** command on a Cisco Catalyst 9800-CL Wireless Controller running software version Cisco IOS XE Cupertino 17.7.1:

```
Device# show license tech support
Smart Licensing Tech Support info

Smart Licensing Status
=====

Smart Licensing is ENABLED

Export Authorization Key:
  Features Authorized:
    <none>

Utility:
  Status: DISABLED
```

```
Smart Licensing Using Policy:
  Status: ENABLED

Account Information:
  Smart Account: <none>
  Virtual Account: <none>

Data Privacy:
  Sending Hostname: yes
  Callhome hostname privacy: DISABLED
  Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license
  Proxy:
    Address: <empty>
    Port: <empty>
    Username: <empty>
    Password: <empty>
  Server Identity Check: True
  VRF: <empty>

Miscellaneous:
  Custom Id: <empty>

Policy:
  Policy in use: Merged from multiple sources.
  Reporting ACK required: yes (CISCO default)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 365 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 90 (CISCO default)
    Reporting frequency (days): 90 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)

Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: <none>
  Reporting push interval: 0 (no reporting) State(1) InPolicy(0)
  Next ACK push check: <none>
  Next report push: <none>
  Last report push: <none>
  Last report file write: <none>

License Usage
=====
Handle: 1
  License: air-network-advantage
  Entitlement Tag:
regid.2018-06.com.cisco.DNA_NWstack,1.0_e7244e71-3ad5-4608-8bf0-d12f67c80896
  Description: air-network-advantage
  Count: 0
```

```

Version: 1.0
Status: NOT IN USE(1)
Status time: Oct 05 22:24:24 2021 UTC
Request Time: None
Export status: NOT RESTRICTED
Feature Name: air-network-advantage
Feature Description: air-network-advantage
Enforcement type: NOT ENFORCED
License type: Perpetual
Measurements:
  ENTITLEMENT:
    Interval: 00:15:00
    Current Value: 0
    Current Report: 0          Previous: 0
  Soft Enforced: True

Handle: 2
License: air-dna-advantage
Entitlement Tag: regid.2017-08.com.cisco.AIR-DNA-A,1.0_b6308627-3ab0-4a11-a3d9-586911a0d790

Description: air-dna-advantage
Count: 0
Version: 1.0
Status: NOT IN USE(1)
Status time: Oct 05 22:24:24 2021 UTC
Request Time: None
Export status: NOT RESTRICTED
Feature Name: air-dna-advantage
Feature Description: air-dna-advantage
Enforcement type: NOT ENFORCED
License type: Subscription
Measurements:
  ENTITLEMENT:
    Interval: 00:15:00
    Current Value: 0
    Current Report: 0          Previous: 0
  Soft Enforced: True

Product Information
=====
UDI: PID:C9800-CL-K9,SN:9KGIXIDOXFE

HA UDI List:
  Active:PID:C9800-CL-K9,SN:9KGIXIDOXFE
  Standby:PID:C9800-CL-K9,SN:9UBKZU955E4

Agent Version
=====
Smart Agent for Licensing: 5.3.14_rel/47

Upcoming Scheduled Jobs
=====
Current time: Oct 06 00:38:46 2021 UTC
Daily: Oct 06 21:24:22 2021 UTC (20 hours, 45 minutes, 36 seconds remaining)
Authorization Renewal: Expired Not Rescheduled
Init Flag Check: Expired Not Rescheduled
Reservation configuration mismatch between nodes in HA mode: Expired Not Rescheduled
Start Utility Measurements: Oct 06 00:39:25 2021 UTC (39 seconds remaining)
Send Utility RUM reports: Oct 06 22:24:54 2021 UTC (21 hours, 46 minutes, 8 seconds remaining)
Save unreported RUM Reports: Oct 06 01:24:35 2021 UTC (45 minutes, 49 seconds remaining)
Data Synchronization: Expired Not Rescheduled
External Event: Expired Not Rescheduled
Operational Model: Expired Not Rescheduled

```

```
Communication Statistics:
=====
Communication Level Allowed: INDIRECT
Overall State: Insufficient trust for direct communication
Trust Establishment:
  Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
  Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>
Trust Acknowledgement:
  Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
  Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>
Usage Reporting:
  Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
  Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>
Result Polling:
  Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
  Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>
Authorization Request:
  Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
  Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>
Authorization Confirmation:
  Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
  Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>
Authorization Return:
  Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
  Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>
Trust Sync:
  Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
  Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>
Hello Message:
  Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
  Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>

License Certificates
=====
Production Cert: False
Not registered. No certificates installed
```

```

HA Info
=====
RP Role: Active
Chassis Role: Active
Behavior Role: Active
RMF: True
CF: True
CF State: Stateless
Message Flow Allowed: False

Reservation Info
=====
License reservation: DISABLED

Overall status:
  Active: PID:C9800-CL-K9,SN:9KGIXIDOXFE
    Reservation status: NOT INSTALLED
    Request code: <none>
    Last return code: <none>
    Last Confirmation code: <none>
    Reservation authorization code: <none>
  Standby: PID:C9800-CL-K9,SN:9UBKZU955E4
    Reservation status: NOT INSTALLED
    Request code: <none>
    Last return code: <none>
    Last Confirmation code: <none>
    Reservation authorization code: <none>

Specified license reservations:

Purchased Licenses:
  No Purchase Information Available

Usage Report Summary:
=====
Total: 0, Purged: 0(0)
Total Acknowledged Received: 0, Waiting for Ack: 0(0)
Available to Report: 0 Collecting Data: 0
Maximum Display: 0 In Storage: 0, MIA: 0(0)
Report Module Status: Ready

Other Info
=====
Software ID: regid.2018-05.com.cisco.WLC_9500C,1.0_85665885-b865-4e32-8184-5510412fcb54
Agent State: authorized
TS enable: True
Transport: Smart
  Default URL: https://smartreceiver.cisco.com/licservice/license
Locale: en_US.UTF-8
Debug flags: 0x7
Privacy Send Hostname: True
Privacy Send IP: True
Build type:: Production
sizeof(char) : 1
sizeof(int) : 4
sizeof(long) : 4
sizeof(char *): 8
sizeof(time_t): 4
sizeof(size_t): 8
Endian: Big
Write Erase Occurred: False
XOS version: 0.12.0.0
Config Persist Received: False
Message Version: 1.3

```

```
connect_info.name: <empty>
connect_info.version: <empty>
connect_info.additional: <empty>
connect_info.prod: False
connect_info.capabilities: <empty>
agent.capabilities: UTILITY, DLC, AppHA, MULTITIER, EXPORT_2, OK_TRY_AGAIN
Check Point Interface: True
Config Management Interface: False
License Map Interface: True
HA Interface: True
Trusted Store Interface: True
Platform Data Interface: True
Crypto Version 2 Interface: False
SAPuginMgmtInterfaceMutex: True
SAPuginMgmtIPDomainName: True
SmartTransportVRFSupport: True
SmartAgentClientWaitForServer: 2000
SmartAgentCmReTrySend: True
SmartAgentClientIsUnified: True
SmartAgentCmClient: True
SmartAgentClientName: UnifiedClient
builtInEncryption: True
enableOnInit: True
routingReadyByEvent: True
systemInitByEvent: True
SmartTransportServerIdCheck: True
SmartTransportProxySupport: True
SmartAgentPolicyDisplayFormat: 0
SmartAgentReportOnUpgrade: False
SmartAgentIndividualRUMEncrypt: 2
SmartAgentMaxRumMemory: 2
SmartAgentConcurrentThreadMax: 10
SmartAgentPolicyControllerModel: False
SmartAgentPolicyModel: True
SmartAgentFederalLicense: True
SmartAgentMultiTenant: False
attr365DayEvalSyslog: True
checkPointWriteOnly: False
SmartAgentDelayCertValidation: False
enableByDefault: False
conversionAutomatic: True
conversionAllowed: False
storageEncryptDisable: False
storageLoadUnencryptedDisable: False
TSPluginDisable: False
bypassUDICheck: False
loggingAddTStamp: False
loggingAddTid: True
HighAvailabilityOverrideEvent: UnknownPlatformEvent
platformIndependentOverrideEvent: UnknownPlatformEvent
platformOverrideEvent: UnknownPlatformEvent
WaitForHaRole: False
standbyIsHot: True
chkPtType: 2
delayCommInit: False
roleByEvent: True
maxTraceLength: 150
traceAlwaysOn: True
debugFlags: 0
Event log max size: 5120 KB
Event log current size: 3 KB
P:C9800-CL-K9,S:9KGIXIDOXFE: No Trust Data
P:C9800-CL-K9,S:9UBKZU955E4: No Trust Data
Overall Trust: No ID
```

```

Clock sync-ed with NTP: True

Platform Provided Mapping Table
=====
C9800-CL-K9: Total licenses found: 5
Enforced Licenses:
P:C9800-CL-K9,S:9KGIXIDOXFE:
  No PD enforced licenses
P:C9800-CL-K9,S:9UBKZU955E4:
  No PD enforced licenses

```

Example (Smart Licensing Using Policy)

The following is sample output from the **show license tech support** command.

```

Device# show license tech support

Smart Licensing Tech Support info

Smart Licensing Status
=====

Smart Licensing is ENABLED
License Reservation is ENABLED

Registration:
Status: REGISTERED - SPECIFIC LICENSE RESERVATION
Export-Controlled Functionality: ALLOWED
Initial Registration: SUCCEEDED on Nov 02 03:16:01 2020 IST

License Authorization:
Status: AUTHORIZED - RESERVED on Nov 02 03:16:01 2020 IST

Export Authorization Key:
Features Authorized:
  <none>

Utility:
Status: DISABLED

Data Privacy:
Sending Hostname: yes
Callhome hostname privacy: DISABLED
Smart Licensing hostname privacy: DISABLED
Version privacy: DISABLED

Transport:
Type: Smart
URL: https://smartreceiver.cisco.com/licservice/license

Evaluation Period:
Evaluation Mode: Not In Use
Evaluation Period Remaining: 89 days, 23 hours, 42 minutes, 47 seconds

License Usage
=====
Handle: 1
License: AP Perpetual Networkstack Advantage
Entitlement tag:
regid.2018-06.com.cisco.DNA_NWStack,1.0_e7244e71-3ad5-4608-8bf0-d12f67c80896
Description: AP Perpetual Network Stack entitled with DNA-A
Count: 1
Version: 1.0

```



```
Status: AUTHORIZED(3)
Status time: Nov 02 03:16:01 2020 IST
Request Time: Nov 02 02:55:34 2020 IST
Export status: NOT RESTRICTED
Soft Enforced: True
```

Handle: 2

```
License: Aironet DNA Advantage Term Licenses
Entitlement tag: regid.2017-08.com.cisco.AIR-DNA-A,1.0_b6308627-3ab0-4a11-a3d9-586911a0d790
```

```
Description: DNA Advantage for Wireless
Count: 1
Version: 1.0
Status: AUTHORIZED(3)
Status time: Nov 02 03:16:01 2020 IST
Request Time: Nov 02 02:55:34 2020 IST
Export status: NOT RESTRICTED
Soft Enforced: True
```

Product Information

=====

UDI: PID:C9800-CL-K9,SN:93BBAH93MGS

HA UDI List:

```
Active:PID:C9800-CL-K9,SN:93BBAH93MGS
Standby:PID:C9800-CL-K9,SN:9XECPSUU4XN
```

Agent Version

=====

Smart Agent for Licensing: 4.8.7_rel/52

Upcoming Scheduled Jobs

=====

```
Current time: Nov 02 03:17:23 2020 IST
Daily: Nov 03 02:47:04 2020 IST (23 hours, 29 minutes, 41 seconds remaining)
Certificate Renewal: Not Available
Certificate Expiration Check: Not Available
Authorization Renewal: Not Available
Authorization Expiration Check: Not Available
Init Flag Check: Not Available
Evaluation Expiration Check: Not Available
Ack Expiration Check: Not Available
Evaluation Expiration Warning: Not Available
IdCert Expiration Warning: Not Available
Reservation request in progress warning: Not Available
Reservation configuration mismatch between nodes in HA mode: Nov 09 03:16:30 2020 IST (6
days, 23 hours, 59 minutes, 7 seconds remaining)
Endpoint Report Request: Not Available
```

License Certificates

=====

```
Production Cert: True
Not registered. No certificates installed
```

HA Info

=====

```
RP Role: Active
Chassis Role: Active
Behavior Role: Active
RMF: True
CF: True
CF State: Stateless
Message Flow Allowed: False
```



```

License type: TERM
  Start Date: 2020-OCT-14 UTC
  End Date: 2021-APR-12 UTC
  Term Count: 10
  Subscription ID: <none>
AP Perpetual Networkstack Advantage (DNA_NWStack):
Description: AP Perpetual Network Stack entitled with DNA-A
Total reserved count: 20
Term information:
  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
    License type: TERM
      Start Date: 2020-OCT-14 UTC
      End Date: 2021-APR-12 UTC
      Term Count: 5
      Subscription ID: <none>
    License type: TERM
      Start Date: 2020-JUN-18 UTC
      End Date: 2020-DEC-15 UTC
      Term Count: 5
      Subscription ID: <none>
  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
    License type: TERM
      Start Date: 2020-OCT-14 UTC
      End Date: 2021-APR-12 UTC
      Term Count: 10
      Subscription ID: <none>

```

Other Info

=====

```

Software ID: regid.2018-05.com.cisco.WLC_9500C,1.0_85665885-b865-4e32-8184-5510412fcb54
Agent State: authorized
TS enable: True
Transport: Smart
  Default URL: https://smartreceiver.cisco.com/licservice/license
Locale: en_US.UTF-8
Debug flags: 0x7
Privacy Send Hostname: True
Privacy Send IP: True
Build type:: Production
sizeof(char)   : 1
sizeof(int)    : 4
sizeof(long)   : 4
sizeof(char *) : 8
sizeof(time_t) : 4
sizeof(size_t) : 8
Endian: Big
Write Erase Occurred: False
XOS version: 0.12.0.0
Config Persist Received: False
Message Version: 1.3
connect_info.name: <empty>
connect_info.version: <empty>
connect_info.additional: <empty>
connect_info.prod: False
connect_info.capabilities: <empty>
agent.capabilities: UTILITY, DLC, AppHA, MULTITIER, EXPORT_2, OK_TRY_AGAIN
SmartAgentClientWaitForServer: 2000
SmartAgentCmReTrySend: True
SmartAgentClientIsUnified: True
SmartAgentCmClient: True
SmartAgentClientName: UnifiedClient
builtInEncryption: True
enableOnInit: True
routingReadyByEvent: True

```

```
systemInitByEvent: True
SmartAgentFederalLicense: True
SmartAgent_Crypto_Exit_CB: 0x55B353357A20
SmartAgent_Crypto_Start_CB: 0x55B353357A10
SmartAgentMultiTenant: False
attr365DayEvalSyslog: True
checkPointWriteOnly: False
SmartAgentDelayCertValidation: False
enableByDefault: False
conversionAutomatic: True
conversionAllowed: False
storageEncryptDisable: False
storageLoadUnencryptedDisable: False
TSPluginDisable: False
bypassUDICheck: False
loggingAddTStamp: False
loggingAddTid: True
platformOverrideEvent: UnknownPlatformEvent
WaitForHaRole: False
standbyIsHot: True
chkPtType: 2
delayCommInit: False
roleByEvent: True
maxTraceLength: 150
traceAlwaysOn: True
debugFlags: 0
Event log max size: 5120 KB
Event log current size: 21 KB
```

```
Platform Provided Mapping Table
=====
<empty>
```

show license udi

To display Unique Device Identifier (UDI) information for a product instance, enter the **show license udi** command in privileged EXEC mode. In a High Availability set-up, the output displays UDI information for all connected product instances.

show license udi

Syntax Description

This command has no keywords or arguments

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 | This command continues to be available with the introduction of Smart Licensing Using Policy. |

Usage Guidelines

Smart Licensing Using Policy: If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2a or a later release, command output displays fields pertinent to Smart Licensing Using Policy.

Smart Licensing: If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing.

Examples

[show license udi with Standalone Product Instance, on page 285](#)

[show license udi with Active and Standby, on page 285](#)

show license udi with Standalone Product Instance

The following is sample output from the **show license udi** command on a standalone product instance.

```
Device# show license udi
UDI: PID:C9800-L-F-K9,SN:FCW2323W016
```

show license udi with Active and Standby

The following is sample output from the **show license udi** command in a High Availability set-up where an active and a standby product instances exist. UDI information is displayed for both.

```
Device# show license udi
UDI: PID:C9800-CL-K9,SN:93BBAH93MGS
HA UDI List:
  Active:PID:C9800-CL-K9,SN:93BBAH93MGS
  Standby:PID:C9800-CL-K9,SN:9XECPSUU4XN
```

show license usage

To display license usage information such as status, a count of licenses being used, and enforcement type, enter the **show license usage** command in privileged EXEC mode.

show license usage

| | |
|---------------------------|---|
| Syntax Description | This command has no keywords or arguments |
|---------------------------|---|

| | |
|----------------------|-----------------|
| Command Modes | Privileged EXEC |
|----------------------|-----------------|

| Command History | Release | Modification |
|-----------------|---|--|
| | This command was introduced in a release earlier than Cisco IOS XE Amsterdam 17.3.2 | This command was introduced. |
| | Cisco IOS XE Amsterdam 17.3.2a | Command output was updated to reflect new fields that are applicable to Smart Licensing Using Policy. This includes the <code>Status</code> , <code>Enforcement type</code> fields. Command output was also updated to remove reservation related information, authorization status information, and export status information. |

| | |
|-------------------------|---|
| Usage Guidelines | Smart Licensing Using Policy: If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2a or a later release, command output displays fields pertinent to Smart Licensing Using Policy. |
|-------------------------|---|

Smart Licensing: If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing.

Examples

See [Table 14: show license usage Field Descriptions, on page 286](#) for information about fields shown in the display.

[show license usage with unenforced licenses \(Smart Licensing Using Policy\), on page 287](#)

[show license usage with unenforced SLR licenses \(Smart Licensing Using Policy\), on page 288](#)

Table 14: show license usage Field Descriptions

| Field | Description |
|-----------------------------------|--|
| License Authorization: Status: | Displays overall authorization status. |
| (): | Name of the license as in CSSM. If this license is one that requires an authorization code, the name of the license and the code. |

| Field | Description |
|--------------------------|--|
| Description | Description of the license as in CSSM. |
| Count | License count. If the license is not in-use, the count is reflected as zero. |
| Version | Version. |
| Status | License status can be one of the following <ul style="list-style-type: none"> • In-Use: Valid license, and in-use. • Not In-Use • Not Authorized: Means that the license requires installation of S... more information, see |
| Export Status: | Indicates if this license is export-controlled or not. Accordingly, one of the following is displayed: <ul style="list-style-type: none"> • RESTRICTED - ALLOWED • RESTRICTED - NOT ALLOWED • NOT RESTRICTED |
| Feature name | Name of the feature that uses this license. |
| Feature Description: | Description of the feature that uses this license. |
| Utility Subscription id: | ID Not applicable, because the corresponding configuration option is not |
| Enforcement type | Enforcement type status for the license. This may be one of the following: <ul style="list-style-type: none"> • ENFORCED • NOT ENFORCED • EXPORT RESTRICTED - ALLOWED • EXPORT RESTRICTED - NOT ALLOWED For more information about enforcement types, see <link tbd> |

show license usage with unenforced licenses (Smart Licensing Using Policy)

The following is sample output of the **show license usage** command. Unenforced licenses are in-use here.

```
Device# show license usage

License Authorization:
  Status: Not Applicable

air-network-essentials (DNA_NWSTACK_E):
  Description: air-network-essentials
  Count: 1
  Version: 1.0
```

```

Status: IN USE
Export status: NOT RESTRICTED
Feature Name: air-network-essentials
Feature Description: air-network-essentials
Enforcement type: NOT ENFORCED
License type: Perpetual

air-dna-essentials (AIR-DNA-E):
Description: air-dna-essentials
Count: 1
Version: 1.0
Status: IN USE
Export status: NOT RESTRICTED
Feature Name: air-dna-essentials
Feature Description: air-dna-essentials
Enforcement type: NOT ENFORCED
License type: Perpetual

```

show license usage with unenforced SLR licenses (Smart Licensing Using Policy)

The following is sample output of the **show license usage** command. Migrated SLR licenses are in-use here:

```

Device# show license usage

air-network-advantage (DNA_NWStack):
Description: air-network-advantage
Count: 1
Version: 1.0
Status: IN USE
Export status: NOT RESTRICTED
Feature Name: air-network-advantage
Feature Description: air-network-advantage
Enforcement type: NOT ENFORCED
License type: Perpetual
Reservation:
  Reservation status: SPECIFIC INSTALLED
  Total reserved count: 20

air-dna-advantage (AIR-DNA-A):
Description: air-dna-advantage
Count: 1
Version: 1.0
Status: IN USE
Export status: NOT RESTRICTED
Feature Name: air-dna-advantage
Feature Description: air-dna-advantage
Enforcement type: NOT ENFORCED
License type: Perpetual
Reservation:
  Reservation status: SPECIFIC INSTALLED
  Total reserved count: 20

```


show platform software rif-mgr chassis active R0 resource-status

To verify the Redundancy Port Interface (RIF) resource status in an active instance, use the **show platform software rif-mgr chassis active R0 resource-status** command.

show platform software rif-mgr chassis active R0 resource-status

| Syntax Description | Parameter | Description |
|--------------------|------------------------|---|
| | rif-mgr | Displays information about the RIF manager. |
| | chassis | Displays information about the chassis. |
| | active | Specifies the Active instance. |
| | R0 | Specifies the Route-Processor slot 0. |
| | resource-status | Displays the resource status. |

Command Default None

Command Modes Privileged EXEC (#)

| Command History | Release | Modification |
|-----------------|-------------------------------|------------------------------|
| | Cisco IOS XE Bengaluru 17.6.1 | This command was introduced. |

Usage Guidelines The RIF resource status displays the RP status, RMI status, Current Chassis State, and Peer Chassis State.

Example

The following example shows how to verify the RIF resource status in active instance:

```
Device# show platform software rif-mgr chassis active R0 resource-status
RIF Resource Status

RP Status           : Up
RMI Status          : Up
Current Chassis State : Active
Peer Chassis State  : Standby
```

show platform software rif-mgr chassis standby R0 resource-status

To verify the Redundancy Port Interface (RIF) resource status in a standby instance, use the **show platform software rif-mgr chassis standby R0 resource-status** command.

show platform software rif-mgr chassis standby R0 resource-status

| Syntax Description | Command | Description |
|--------------------|------------------------|---|
| | rif-mgr | Displays information about the RIF manager. |
| | chassis | Displays information about the chassis. |
| | standby | Specifies the Standby instance. |
| | R0 | Specifies the Route-Processor slot 0. |
| | resource-status | Displays the resource status. |

Command Default None

Command Modes Privileged EXEC (#)

| Command History | Release | Modification |
|-----------------|-------------------------------|------------------------------|
| | Cisco IOS XE Bengaluru 17.6.1 | This command was introduced. |

Usage Guidelines The RIF resource status displays the RP status, RMI status, Current Chassis State, and Peer Chassis State.

Example

The following example shows how to verify the RIF resource status in standby instance:

```
Device# show platform software rif-mgr chassis standby R0 resource-status
RIF Resource Status

  RP Status           : Up
  RMI Status          : Up
  Current Chassis State : Standby
  Peer Chassis State   : Active
```

show platform software rif-mgr chassis active R0 rmi-connection-details

To verify the RMI link re-establishment count and the time since it is Up or Down in an active instance, use the **show platform software rif-mgr chassis active R0 rmi-connection-details** command.

show platform software rif-mgr chassis active R0 rmi-connection-details

| Syntax Description | Command | Description |
|--------------------|-------------------------------|---|
| | rif-mgr | Displays information about the RIF manager. |
| | chassis | Displays information about the chassis. |
| | active | Specifies the Active instance. |
| | R0 | Specifies the Route-Processor slot 0. |
| | rmi-connection-details | Displays the RMI connection details. |

Command Default None

Command Modes Privileged EXEC (#)

| Command History | Release | Modification |
|-----------------|-------------------------------|------------------------------|
| | Cisco IOS XE Bengaluru 17.6.1 | This command was introduced. |

Examples

The following example shows how to verify the RMI link re-establishment count and the time since it is Up in an active instance:

```
Device# show platform software rif-mgr chassis active R0 rmi-connection-details
RMI Connection Details
  RMI Link re-establish count : 2
  RMI Link Uptime             : 21 hours 8 minutes 43 seconds
  RMI Link Upsince            : 08/05/2021 13:46:01
```

The following example shows how to verify the RMI link re-establishment count and the time since it is Down in an active instance:

```
Device# show platform software rif-mgr chassis active R0 rmi-connection-details
RMI Connection Details
  RMI Link re-establish count : 1
  RMI Link Downtime           : 28 seconds
  RMI Link Downsince          : 07/16/2021 03:19:11
```

show platform software rif-mgr chassis standby R0 rmi-connection-details

To verify the RMI link re-establishment count and the time since it is Up or Down in a standby instance, use the **show platform software rif-mgr chassis standby R0 rmi-connection-details** command.

show platform software rif-mgr chassis standby R0 rmi-connection-details

| | | |
|---------------------------|-------------------------------|---|
| Syntax Description | rif-mgr | Displays information about the RIF manager. |
| | chassis | Displays information about the chassis. |
| | standby | Specifies the Standby instance. |
| | R0 | Specifies the Route-Processor slot 0. |
| | rmi-connection-details | Displays the RMI connection details. |
| Command Default | None | |
| Command Modes | Privileged EXEC (#) | |
| Command History | Release | Modification |
| | Cisco IOS XE Bengaluru 17.6.1 | This command was introduced. |

Examples

The following example shows how to verify the RMI link re-establishment count and the time since it is Up in a standby instance:

```
Device# show platform software rif-mgr chassis standby R0 rmi-connection-details
RMI Connection Details
  RMI Link re-establish count : 1
  RMI Link Uptime             : 1 hour 39 minute 9 seconds
  RMI Link Upsince            : 07/16/2021 01:31:41
```

The following example shows how to verify the RMI link re-establishment count and the time since it is Down in a standby instance:

```
Device# show platform software rif-mgr chassis standby R0 rmi-connection-details
RMI Connection Details
  RMI Link re-establish count : 1
  RMI Link Downtime          : 22 seconds
  RMI Link Downsince         : 07/16/2021 03:19:17
```

show platform software rif-mgr chassis active R0 rp-connection-details

To verify the RP link re-establishment count and the time since it is UP or Down in an active instance, use the **show platform software rif-mgr chassis active R0 rp-connection-details** command.

show platform software rif-mgr chassis active R0 rp-connection-details

| Syntax Description | Parameter | Description |
|--------------------|------------------------------|---|
| | rif-mgr | Displays information about the RIF manager. |
| | chassis | Displays information about the chassis. |
| | active | Specifies the Active instance. |
| | R0 | Specifies the Route-Processor slot 0. |
| | rp-connection-details | Displays the RP connection details. |

Command Default None

Command Modes Privileged EXEC (#)

| Command History | Release | Modification |
|-----------------|-------------------------------|------------------------------|
| | Cisco IOS XE Bengaluru 17.6.1 | This command was introduced. |

Examples

The following example shows how to verify the RP link re-establishment count and the time since it is UP for days in an active instance:

```
Device# show platform software rif-mgr chassis active R0 rp-connection-details
RP Connection Details
  RP Connection Uptime   : 12 days 17 hours 1 minute 39 seconds
  RP Connection Upsince  : 07/03/2021 07:06:20
```

The following example shows how to verify the RP link re-establishment count and the time since it is Down in an active instance:

```
Device# show platform software rif-mgr chassis active R0 rp-connection-details
RP Connection Details
  RP Connection Downtime   : 4 seconds
  RP Connection Downsince  : 07/16/2021 03:33:04
```

show platform software rif-mgr chassis standby R0 rp-connection-details

To verify the RP link re-establishment count and the time since it is UP or Down in a standby instance, use the **show platform software rif-mgr chassis standby R0 rp-connection-details** command.

show platform software rif-mgr chassis standby R0 rp-connection-details

| | | |
|---------------------------|-------------------------------|---|
| Syntax Description | rif-mgr | Displays information about the RIF manager. |
| | chassis | Displays information about the chassis. |
| | standby | Specifies the Standby instance. |
| | R0 | Specifies the Route-Processor slot 0. |
| | rp-connection-details | Displays the RP connection details. |
| Command Default | None | |
| Command Modes | Privileged EXEC (#) | |
| Command History | Release | Modification |
| | Cisco IOS XE Bengaluru 17.6.1 | This command was introduced. |

Examples

The following example shows how to verify the RP link re-establishment count and the time since it is UP in a standby instance:

```
Device# show platform software rif-mgr chassis standby R0 rp-connection-details
RP Connection Details
  RP Connection Uptime   : 12 days 17 hours 2 minutes 1 second
  RP Connection Upsince  : 07/03/2021 07:05:58
```

The following example shows how to verify the RP link re-establishment count and the time since it is Down in a standby instance:

```
Device# show platform software rif-mgr chassis standby R0 rp-connection-details
RP Connection Details
  RP Connection Downtime   : 22 seconds
  RP Connection Downsince  : 07/16/2021 03:19:17
```

show platform software rif-mgr chassis active R0 rif-stk-internal-stats

To verify the RIF and stack manager internal statistics in an active instance, use the **show platform software rif-mgr chassis active R0 rif-stk-internal-stats** command.

show platform software rif-mgr chassis active R0 rif-stk-internal-stats

| Syntax Description | Parameter | Description |
|--------------------|-------------------------------|---|
| | rif-mgr | Displays information about the RIF manager. |
| | chassis | Displays information about the chassis. |
| | active | Specifies the Active instance. |
| | R0 | Specifies the Route-Processor slot 0. |
| | rif-stk-internal-stats | Displays the RIF and stack manager internal statistics. |

Command Default None

Command Modes Privileged EXEC (#)

| Command History | Release | Modification |
|-----------------|-------------------------------|------------------------------|
| | Cisco IOS XE Bengaluru 17.6.1 | This command was introduced. |

Example

The following example shows how to verify the RIF and stack manager internal statistics in an active instance:

```
Device# show platform software rif-mgr chassis active R0 rif-stk-internal-stats
RIF Stack Manager internal stats

Stack-mgr reported RP down           : False
DAD link status reported to Stack-Mgr : True
```

show platform software rif-mgr chassis standby R0 rif-stk-internal-stats

To verify the RIF and stack manager internal statistics in a standby instance, use the **show platform software rif-mgr chassis standby R0 rif-stk-internal-stats** command.

show platform software rif-mgr chassis standby R0 rif-stk-internal-stats

| Syntax Description | Parameter | Description |
|--------------------|-------------------------------|---|
| | rif-mgr | Displays information about the RIF manager. |
| | chassis | Displays information about the chassis. |
| | standby | Specifies the Standby instance. |
| | R0 | Specifies the Route-Processor slot 0. |
| | rif-stk-internal-stats | Displays the RIF and stack manager internal statistics. |
| Command Default | None | |
| Command Modes | Privileged EXEC (#) | |
| Command History | Release | Modification |
| | Cisco IOS XE Bengaluru 17.6.1 | This command was introduced. |

Example

The following example shows how to verify the RIF and stack manager internal statistics in a standby instance:

```
Device# show platform software rif-mgr chassis standby R0 rif-stk-internal-stats
RIF Stack Manager internal stats

Stack-mgr reported RP down           : False
DAD link status reported to Stack-Mgr : True
```


show platform software rif-mgr chassis active R0 lmp-statistics

To verify the number of packets sent or received for each type in an active instance, use the **show platform software rif-mgr chassis active R0 lmp-statistics** command.

show platform software rif-mgr chassis active R0 lmp-statistics

| Syntax Description | Parameter | Description |
|--------------------|-----------------------|---|
| | rif-mgr | Displays information about the RIF manager. |
| | chassis | Displays information about the chassis. |
| | active | Specifies the Active instance. |
| | R0 | Specifies the Route-Processor slot 0. |
| | lmp-statistics | Displays the LMP statistics. |

Command Default None

Command Modes Privileged EXEC (#)

| Command History | Release | Modification |
|-----------------|-------------------------------|------------------------------|
| | Cisco IOS XE Bengaluru 17.6.1 | This command was introduced. |

Example

The following example shows how to verify the number of packets sent or received for each type in an active instance:

```
Device# show platform software rif-mgr chassis active R0 lmp-statistics
LMP Statistics

Info Type Sent                : 6
Solicit Info Type Sent        : 0
Unsolicit Info Type Sent      : 6
Reload Type Sent              : 0
Recovery Type Sent            : 1
Gateway Info Type Sent        : 0
Enquiry Type Sent             : 0
Solicit Enquiry Type Sent     : 0
Unsolicit Enquiry Type Sent   : 0

Info Type Received            : 5
Solicit Info Type Received    : 2
Unsolicit Info Type Received  : 3
Reload Type Received          : 0
Recovery Type Received        : 0
Gateway Info Type Received    : 4
Enquiry Type Received         : 0
Solicit Enquiry Type Received : 0
Unsolicit Enquiry Type Received : 0
```

show platform software rif-mgr chassis standby R0 lmp-statistics

To verify the number of packets sent or received for each type in a standby instance, use the **show platform software rif-mgr chassis standby R0 lmp-statistics** command.

show platform software rif-mgr chassis standby R0 lmp-statistics

| Syntax Description | Parameter | Description |
|--------------------|-----------------------|---|
| | rif-mgr | Displays information about the RIF manager. |
| | chassis | Displays information about the chassis. |
| | standby | Specifies the Standby instance. |
| | R0 | Specifies the Route-Processor slot 0. |
| | lmp-statistics | Displays the LMP statistics. |

Command Default None

Command Modes Privileged EXEC (#)

| Command History | Release | Modification |
|-----------------|-------------------------------|------------------------------|
| | Cisco IOS XE Bengaluru 17.6.1 | This command was introduced. |

Example

The following example shows how to verify the number of packets sent or received for each type in a standby instance:

```
Device# show platform software rif-mgr chassis standby R0 lmp-statistics
LMP Statistics

Info Type Sent                : 6
Solicit Info Type Sent        : 0
Unsolicit Info Type Sent      : 6
Reload Type Sent              : 0
Recovery Type Sent            : 0
Gateway Info Type Sent        : 4
Enquiry Type Sent             : 0
Solicit Enquiry Type Sent     : 0
Unsolicit Enquiry Type Sent   : 0

Info Type Received            : 5
Solicit Info Type Received    : 3
Unsolicit Info Type Received  : 2
Reload Type Received          : 0
Recovery Type Received        : 1
Gateway Info Type Received    : 0
Enquiry Type Received         : 0
```

```
Solicit Enquiry Type Received : 0  
Unsolicit Enquiry Type Received : 0
```

show platform software sl-infra

To display troubleshooting information and for debugging, enter the **show platform software sl-infra** command in privileged EXEC mode. The output of this command is used by the technical support team, for troubleshooting and debugging.

show platform software sl-infra { **all** | **current** | **debug** | **stored** }

Syntax Description

| | |
|----------------|--|
| all | Displays current, debugging, and stored information. |
| current | Displays current license-related information. |
| debug | Enables debugging |
| stored | Displays information that is stored on the product instance. |

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|--------------------------------|------------------------------|
| Cisco IOS XE Amsterdam 17.3.2a | This command was introduced. |

Usage Guidelines

When you encounter an error message that you are not able to resolve, along with a copy of the message that appears on the console or in the system log, provide your Cisco technical support representative with sample output of these commands: **show license tech support**, **show license history message**, and the **show platform software sl-infra all** privileged EXEC commands.

show platform software tls client summary

To view the TLS client summary details, use the **show platform software tls client summary** command.

show platform software tls client summary

| | |
|---------------------------|--|
| Syntax Description | This command has no keywords or arguments. |
|---------------------------|--|

| | |
|----------------------|----------------------|
| Command Modes | Global configuration |
|----------------------|----------------------|

| Command History | Release | Modification |
|------------------------|-------------------------------|------------------------------|
| | Cisco IOS XE Bengaluru 17.6.1 | This command was introduced. |

Examples

This example shows how to view the TLS client summary details:

```
Device # show platform software tls client summary
```

| Name | ID | Gateway | Port | Auth | Trustpoint | DPD Time | Rekey Time | Retry Time |
|-------|----|---------|------|------|------------|----------|------------|------------|
| ----- | | | | | | | | |
| fqdn | 0 | | 8443 | PSK | N/A | 60 | 300 | 20 |

show platform software client detail

To display a summary of TLS client session detail, session statistics, tunnel statistics, and DNS counters, use the **show platform software client detail** command.

show platform software client detail

Syntax Description This command has no keywords or arguments.

Command Modes Global configuration

Command History

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

Examples

This example shows how to view the TLS client summary details:

```
Device # show platform software client detail

TLS Client           : Session Detail
Session Name        : fqdn
FQDN resolved IP    : 10.194.234.149
ID                  : 0
Created             : 04/20/21 00:36:42
Updated            : 04/22/21 05:56:03
State              : Up (Rekey)
Up Time            : 04/21/21 20:30:21 ( 9 hours 25 minutes 45 seconds )
Down Time          : 04/21/21 20:30:01
Rekey Time         : 04/22/21 05:55:51 ( 15 seconds )

TLS Session Statistics

Up Notifications    : 3
Down Notifications  : 2
Rekey Notifications : 636
DP State Updates    : 0
DPD Cleanups        : 0

Packets From      Packets To  Packet Errors To  Bytes From      Bytes To
-----
BinOS              80             0                  0                0
IOSd               0              0                  0                0

TLS Client         0              0                  0                0

TLS Tunnel Statistics
Type              Tx Packets      Rx Packets
-----
Total             0               80
CSTP Ctrl        3836            3836
CSTP Data        80              0

Type              Requests        Responses
-----
```

```
CSTP Cfg          639          639
CSTP DPD          3197         3197

Invalid CSTP Rx      : 0
Injected Packet Success : 0
Injected Packet Failed : 0
Consumed Packets     : 0

TLS Tunnel DNS Counters
DNS Resolve Request Success Count : 641
DNS Resolve Request Failure Count  : 0
DNS Resolve Success Count          : 639
DNS Resolve Failure Count          : 2
```

show platform software tls statistics

To view the TLS client global statistic details, use the **show platform software tls statistics** command.

show platform software tls statistics

Syntax Description This command has no keywords or arguments.

Command Modes Global configuration

Command History

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

Examples This example shows how to view the TLS client summary details:

```
Device # show platform software tls statistics

TLS Client - Global Statistics
Session Statistics
Up/Down           : 5/2
Rekeys            : 636
DP Updates        : 0
DPD Cleanups      : 0

Packets From      Packets To      Packet Errors To  Bytes From      Bytes To
-----
BinOS              85                0                  0                0
IOSd 0             0                  0                  0                0
TLS Client 0       0                  0                  0                0

Tunnel Statistics
SSL Handshake Init/Done : 641/641
TCP Connection Req/Done : 641/641

Tunnel Packets
Rx/Tx                : 85/0
Injected / Failed    : 0/0
Consumed              : 0

CSTP Packets
Control Rx/Tx        : 3839 / 3839
Data Rx/Tx           : 0 / 85
Config Req/Resp      : 641 / 641
DPD Req/Resp         : 3198 / 3198
Invalid Rx           : 0

FQDN Counters
Req/Resp/Success     : 0/0/0

NAT Counters
Transalte In/Out     : 0/0
Ignore In/Out        : 0/0
Failed                : 0
Invalid              : 0
```



```
No Entry           : 0
Unsupported        : 0
```

Internal Counters

| Type | Allocated | Freed |
|--------|-----------|-------|
| EV | 1299 | 1295 |
| Tunnel | 5 | 4 |
| Conn | 643 | 642 |
| Sess | 3 | 2 |

Config Message Related Counters

| Type | Success | Failed |
|--------|---------|--------|
| Create | 3 | 0 |
| Delete | 2 | 0 |

show platform software tls session summary

To view the tls client session summary, use the **show platform software tls session summary** command.

show platform software tls session summary

Syntax Description

This command has no keywords or arguments.

Command Modes

Global configuration

Command History

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

Examples

This example shows how to view the TLS client summary details:

```
Device # show platform software tls session summary
```

```
TLS Client - Session Summary
```

| Name | ID | Created | State | Since | Elapsed |
|------|----|-------------------|-------|-------------------|-------------------------------|
| fqdn | 0 | 04/20/21 00:36:42 | Up | 04/21/21 20:30:21 | 9 hours 26 minutes 44 seconds |

show product-analytics kpi report

To display the details of a particular product analytics engine report, use the **show product-analytics kpi report** command.

show product-analytics kpi report

| Syntax Description | <i>report-id</i> Report identifier. | | | | |
|-----------------------------|---|---------|--------------|-----------------------------|------------------------------|
| Command Default | None | | | | |
| Command Modes | Privileged EXEC (#) | | | | |
| Command History | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Dublin 17.10.1</td> <td>This command was introduced.</td> </tr> </tbody> </table> | Release | Modification | Cisco IOS XE Dublin 17.10.1 | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE Dublin 17.10.1 | This command was introduced. | | | | |

Examples

The following example displays the details of a particular product analytics engine report:

```
Device# show product-analytics kpi report <report-id>

Product Analytics Engine KPIs

Report ID       : 1662422400
Computed at    : 09/06/2022 00:00:00
KPI Name       : ap_mode
.
.
Report ID       : 1662422400
Computed at    : 09/06/2022 00:00:00
KPI Name       : clients_distinct_wireless_lua
KPI Value      : 0
```

show product-analytics kpi summary

To display the product analytics engine report summary, use the **show product-analytics kpi summary** command.

show product-analytics kpi summary

| | |
|---------------------------|--|
| Syntax Description | This command has no keywords or arguments. |
|---------------------------|--|

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

| | |
|----------------------|---------------------|
| Command Modes | Privileged EXEC (#) |
|----------------------|---------------------|

| Command History | Release | Modification |
|------------------------|-----------------------------|------------------------------|
| | Cisco IOS XE Dublin 17.10.1 | This command was introduced. |

Examples

The following example displays the product analytics engine report summary:

```
Device# show product-analytics kpi summary
```

```
Product Analytics Engine KPIs
```

| Time | Report ID | KPI Name |
|---------------------|------------|-------------------------------|
| 09/06/2022 00:00:00 | 1662422400 | ap_mode |
| 09/06/2022 00:00:00 | 1662422400 | ap_type |
| 09/06/2022 00:00:00 | 1662422400 | fra_usage |
| . | | |
| . | | |
| . | | |
| 09/15/2022 00:00:00 | 1663200000 | clients_concurrent_wireless |
| 09/15/2022 00:00:00 | 1663200000 | clients_distinct_wireless_lua |

show product-analytics report detail

To display the product analytics engine report details, use the **show product-analytics report detail** command.

show product-analytics report detail

| | | |
|---------------------------|--|------------------------------|
| Syntax Description | This command has no keywords or arguments. | |
| Command Default | None | |
| Command Modes | Privileged EXEC (#) | |
| Command History | Release | Modification |
| | Cisco IOS XE Dublin 17.10.1 | This command was introduced. |

Examples

The following example displays the product analytics engine report details:

```
Device# show product-analytics report detail
```

```
Product Analytics Engine Reports
```

```
Report ID       : 1662422400
Policy Version  : 17.10.1
Engine Version  : 17.10.1
File version    : 1
Period start    :
Period End      :
Timezone       : 0
```

```
Event History
```

```
Timestamp          #Times  Event                RC Context
-----
09/14/2022 22:15:01.814 1      REPORT_SEND         5 DRAGONFLY
```

```
.
.
.
```

```
Report ID       : 1663200000
Policy Version  : 17.10.1
Engine Version  : 17.10.1
File version    : 1
Period start    :
Period End      :
Timezone       : 0
```

```
Event History
```

```
Timestamp          #Times  Event                RC Context
-----
09/15/2022 00:00:00.836 1      KPI_ADD             0 clients_distinct_wireless_lua
```

show product-analytics report detail

```
09/15/2022 00:00:00.824 1      KPI_ADD      0 client_auth_protocol_lua
09/15/2022 00:00:00.793 1      KPI_ADD      0 clients_concurrent_wireless
09/15/2022 00:00:00.793 1      KPI_ADD      0 network_ssid_count
09/15/2022 00:00:00.793 1      KPI_ADD      0 ap_type
09/15/2022 00:00:00.792 1      KPI_ADD      0 fra_enabled
09/15/2022 00:00:00.792 1      KPI_ADD      0 ap_software_version
09/15/2022 00:00:00.792 1      KPI_ADD      0 ap_mode
09/15/2022 00:00:00.792 1      KPI_ADD      0 fra_usage
09/15/2022 00:00:00.791 1      NEW_REPORT   0
```

show product-analytics stats

To display the product analytics engine statistics and event history, use the **show product-analytics stats** command.

show product-analytics stats

| | | |
|---------------------------|--|------------------------------|
| Syntax Description | This command has no keywords or arguments. | |
| Command Default | None | |
| Command Modes | Privileged EXEC (#) | |
| Command History | Release | Modification |
| | Cisco IOS XE Dublin 17.10.1 | This command was introduced. |

Examples

The following example displays the product analytics engine statistics and event history:

```
Device# show product-analytics stats

Product Analytics Engine Statistics

Policy-Version
File version                : 1
Data-Store
#Writes                     : 941442
Total write time (us)       : 754856891
Average write time (us)    : 801
#Single Writes              : 1890439
Total Single write time (us) : 41098825
Average Single write time (us) : 21
#Queries                    : 737
Total query time (us)      : 4534566
Average query time (us)    : 6152
#Query errors               :

Data-Source
#Periodic reads             : 2195456
Total periodic-read time (us) : 7414384002
Average periodic-read time (us) : 3377
#Periodic read batches     : 3136361
Total periodic-read-batch time (us) : 1826634998
Average periodic-read-batch time (us) : 582
#On-change reads           : 604

KPI
#SQL computatious          : 66
Total SQL KPI compute time (us) : 202907
Average SQL KPI compute time (us) : 3074
#LUA computatious          : 66
Total LUA KPI compute time (us) : 3211022
Average LUA KPI compute time (us) : 48651

Event History
```

| Timestamp | #Times | Event | RC | Context |
|---|----------|-----------------|----|--|
| 09/15/2022 02:18:24.428 | 40323979 | DSRC_PERIOD_RD | 0 | |
| /services;serviceName=ewlc_oper/radio_oper_data | | | | |
| 09/15/2022 01:18:07.561 | 941442 | DST_STORE_END | 0 | |
| 09/15/2022 01:18:07.561 | 941442 | DST_STORE_BEGIN | 0 | |
| 09/15/2022 01:18:07.560 | 941442 | DSRC_NORMALIZE | 0 | rrmRadSlot |
| 09/15/2022 00:00:03.583 | 604 | DSRC_ONCHG_RD | 0 | /services;serviceName=ewlc/wlan_config |

show lisp site detail

To see detailed Locator ID Separation Protocol (LISP) site information on a map server, use the **show lisp site detail** command.

```
show lisp site detail [{eid-table {default | vlan vlan-id | vrf vrf-name } | instance-id id-number |
internal {eid-table {default | vlan vlan-id | vrf vrf-name} | instance-id id-number}]
```

| Syntax Description | Option | Description |
|--------------------|-------------------------------------|---|
| | eid-table | Option to enter the EID table. |
| | default | Shows the information for the default VRF. |
| | vlan <i>vlan-id</i> | Enter the VLAN information. |
| | vrf <i>vrf-name</i> | Enter the VRF name. |
| | instance-id <i>id-number</i> | Enter the EID instance ID. |
| | internal | Shows the site's detailed internal information. |

Command Default None

Command Modes Privileged EXEC

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

Examples

The following example shows how to see detailed Locator ID Separation Protocol (LISP) site information on a map server:

```
Device# show lisp site detail
```

show logging profile wireless end timestamp

To specify log filtering end location timestamp for filtering, use the **show logging profile wireless end timestamp** command.

show logging profile wireless end timestamp *time-stamp*

| | |
|---------------------------|--|
| Syntax Description | <i>time-stamp</i> Time to end the filtering. For example, 2017/02/10 14:41:50.849. |
|---------------------------|--|

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

| | |
|----------------------|---------------------|
| Command Modes | Privileged EXEC (#) |
|----------------------|---------------------|

| Command History | Release | Modification |
|------------------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

| | |
|-------------------------|--|
| Usage Guidelines | Ensure that you enable internal keyword using the show logging profile wireless internal command to get the trace output. |
|-------------------------|--|

Example

The following example shows how to specify log filtering end location timestamp for filtering:

```
Device# show logging profile wireless end timestamp 2017/02/10 14:41:50.849
```

show logging profile wireless filter

To specify filter for logs, use the **show logging profile wireless filter** command.

```
show logging profile wireless filter { ipv4 | mac | string | uuid }
```

Syntax Description

ipv4 Selects logs with specific IP address app context.

mac Selects logs with specific MAC app context.

string Selects logs with specific string app context.

uuid Selects logs with specific Universally Unique Identifier (UUID) app context.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Ensure that you enable **internal** keyword using the **show logging profile wireless internal** command to get the trace output.

Without the **internal** keyword, only customer curated logs are displayed.

Example

The following example shows how to specify filter for logs:

```
Device# show logging profile wireless filter ipv4 10.10.11.1
```

show logging profile wireless fru

To specify field-replaceable unit (FRU) specific commands, use the **show logging profile wireless fru** command.

show logging profile wireless fru {0 {reverse | to-file}} chassis} {0 {reverse | to-file} | chassis }

Syntax Description

| | |
|----------------|--|
| 0 | SPA-Inter-Processor slot 0. |
| reverse | Shows logs in reverse chronological order. |
| to-file | Decodes files stored in disk and write output to file. |
| chassis | Chassis name. |

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Ensure that you enable **internal** keyword using the **show logging profile wireless internal** command to get the trace output.

Without the **internal** keyword, only customer curated logs are displayed.

Example

The following example shows how to specify FRU specific commands:

```
Device# show logging profile wireless fru 0
```

show logging profile wireless internal

To select all the logs, use the **show logging profile wireless internal** command.

show logging profile wireless internal

| | |
|---------------------------|--|
| 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 | Ensure that you enable internal keyword using the show logging profile wireless internal command to get the trace output. |
|-------------------------|---|

Without the **internal** keyword, only customer curated logs are displayed.

Example

The following example shows how to display all the logs:

```
Device# show logging profile wireless internal
```

show logging profile wireless level

To select logs above a specific level, use the **show logging profile wireless level** command.

```
show logging profile wireless level { debug | emergency | error | info | noise | notice | verbose | warning
}
```

| Syntax Description | | |
|--------------------|--------------------------------------|--|
| debug | Selects debug messages. | |
| emergency | Selects emergency possible messages. | |
| error | Selects error messages. | |
| info | Selects informational messages. | |
| noise | Selects maximum possible messages. | |
| notice | Selects notice messages. | |
| verbose | Selects verbose debug messages. | |
| warning | Selects warning messages. | |

Command Default None

Command Modes Privileged EXEC (#)

| Command History | Release | Modification |
|-----------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

Usage Guidelines Ensure that you enable **internal** keyword using the **show logging profile wireless internal** command to get the trace output.

Without the **internal** keyword, only customer curated logs are displayed.

Example

The following example shows how to select logs above a specific level:

```
Device# show logging profile wireless level info
```

show logging profile wireless module

To select logs for specific modules, use the **show logging profile wireless module** command.

```
show logging profile wireless module module-name
```

| Syntax Description | <i>module-name</i> A comma or space separated list of module names. For example, dbal, tdllib or "dbal tdllib". | | | | |
|--------------------------------|--|---------|--------------|--------------------------------|------------------------------|
| Command Default | None | | | | |
| Command Modes | Privileged EXEC (#) | | | | |
| Command History | <table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>Cisco IOS XE Gibraltar 16.10.1</td><td>This command was introduced.</td></tr></tbody></table> | Release | Modification | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. | | | | |
| Usage Guidelines | <p>Ensure that you enable internal keyword using the show logging profile wireless internal command to get the trace output.</p> <p>Without the internal keyword, only customer curated logs are displayed.</p> | | | | |

Example

The following example shows how to select logs for specific modules:

```
Device# show logging profile wireless module dbal
```

show logging profile wireless reverse

To view logs in reverse chronological order, use the **show logging profile wireless reverse** command.

show logging profile wireless reverse

| | |
|---------------------------|--|
| 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 | Ensure that you enable internal keyword using the show logging profile wireless internal command to get the trace output. |
|-------------------------|---|

Without the **internal** keyword, only customer curated logs are displayed.

Example

The following example shows how to view logs in reverse chronological order:

```
Device# show logging profile wireless reverse
```


show logging profile wireless start

To specify log filtering start location, use the **show logging profile wireless start** command.

```
show logging profile wireless start { marker marker | timestamp time-stamp }
```

Syntax Description

| | |
|------------------|---|
| marker | The marker to start filtering from. It must match with previously set marker. |
| timestamp | The timestamp for filtering. for example, "2017/02/10 14:41:50.849". |

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Ensure that you enable **internal** keyword using the **show logging profile wireless internal** command to get the trace output.

Without the **internal** keyword, only customer curated logs are displayed.

Example

The following example shows how to specify log filtering start location:

```
Device# show logging profile wireless start timestamp 2017/02/10 14:41:50.849
```

show logging profile wireless switch

To specify the switch to look for logs, use the **show logging profile wireless switch** command.

show logging profile wireless switch { *switch-num* | **active** | **standby** }

Syntax Description

chassis-num Chassis number.

active Selects the active instance.

standby Selects the standby instance.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Ensure that you enable **internal** keyword using the **show logging profile wireless internal** command to get the trace output.

Without the **internal** keyword, only customer curated logs are displayed.

Example

The following example shows how to specify the chassis number to look for logs:

```
Device# show logging profile wireless switch active
```

show logging profile wireless to-file

To decode files stored in disk and write the output to a file, use the **show logging profile wireless to-file** command.

show logging profile wireless to-file *output-file-name*

Syntax Description

output-file-name Output file name. File with this name will be created in the flash memory.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Ensure that you enable **internal** keyword using the **show logging profile wireless internal** command to get the trace output.

Without the **internal** keyword, only customer curated logs are displayed.

Example

The following example shows how to decode files stored in disk and write the output to a file:

```
Device# show logging profile wireless to-file testfile
```

show mdns-sd cache

To view mDNS cache details, use the **show mdns-sd cache** command.

```
show mdns-sd cache { ap-mac mac-address (H.H.H) | client-mac client-mac-address (H.H.H) |
detail | glan-id <1 - 5> | location-group <0 - 4096> | mdns-ap mdns-ap mac address (H.H.H)
| rlan-id <1 - 128> | statistics | type { A-AAAA | PTR | SRV | TXT } | udn
{ <1 - 4294967295> | shared } | wired | wlan-id <0 - 4096> }
```

Syntax Description

| | |
|---|--|
| ap-mac <i>mac-address (H.H.H)</i> | Specifies the AP Ethernet MAC address. |
| client-mac <i>client-mac-address (H.H.H)</i> | Specifies the client MAC address. |
| detail | Specifies the cache in detail. |
| location-group <i><0 - 4096></i> | Specifies the location group. The value range is from 0 to 4096. |
| mdns-ap <i>mdns-ap mac address (H.H.H)</i> | Specifies the cache learnt from a specific mDNS AP. |
| rlan-id <i><1 - 128></i> | Specifies the remote LAN ID. The value range is from 1 - 128. |
| statistics | Specifies the mDNS cache statistics. |
| type | Specifies the mDNS record type. The record types are, A-AAAA, PTR, SRV, and TXT. |
| udn <i><1 - 4294967295></i> | Specifies the UDN ID. The value range is from 1 to 4294967295. |
| shared | Specifies the UDN shared services. |
| wired | Specifies the mDNS services from wired clients. |
| wlan-id <i><0 - 4096></i> | Specifies the WLAN ID. The value range is from 1 to 4096. |

Command Default

None

Command Modes

Privileged EXEC mode

Command History

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

Usage Guidelines

None

Example

The following example shows how to view the mDNS cache details:

```
Device# show mdns-sd cache
```

show mdns-sd cache detail

To view the multicast DNS (mDNS) cache details, use the **show mdns-sd cache detail** command.

show mdns-sd cache detail

| Syntax Description | This command has no keywords or arguments. | | | | |
|--------------------------------|--|---------|--------------|--------------------------------|------------------------------|
| Command Default | None | | | | |
| Command Modes | Privileged EXEC (#) | | | | |
| Command History | <table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>Cisco IOS XE Amsterdam 17.1.1s</td><td>This command was introduced.</td></tr></tbody></table> | Release | Modification | Cisco IOS XE Amsterdam 17.1.1s | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE Amsterdam 17.1.1s | This command was introduced. | | | | |

Example

The following is sample output from the **show mdns-sd cache detail** command:

```
Device# show mdns-sd cache detail

Name: _printer._tcp.local
Type: PTR
TTL: 4500
VLAN: 21
Client MAC: ace2.d3bc.047e
Remaining-Time: 4383
mDNS Service Policy: default-mdns-service-policy
Rdata: HP OfficeJet Pro 8720 [BC047E] (2)._printer._tcp.local
```

show mdns-sd cache upn shared

To view the multicast DNS (mDNS) cache user personal network shared services details, use the **show mdns-sd cache upn shared** command.

show mdns-sd cache upn shared

| | | |
|---------------------------|--|------------------------------|
| Syntax Description | This command has no keywords or arguments. | |
| Command Default | None | |
| Command Modes | Privileged EXEC (#) | |
| Command History | Release | Modification |
| | Cisco IOS XE Amsterdam 17.1.1s | This command was introduced. |

Example

The following is sample output from the **show mdns-sd cache upn shared** command that displays the mDNS cache UPN shared services details:

```
Device# show mdns-sd cache upn shared
```

```

----- PTR Records -----
-----
RECORD-NAME                                TTL      TYPE      ID      CLIENT-MAC
RR-RECORD-DATA
-----
9.1.1.7.5.D.E.F.F.F.C.7.E.2.1.0.0.0.0.0.0  4500     WLAN      2       10e7.c6d5.7119
HP10E7C6D57119-2860.local
_services._dns-sd._udp.local              4500     WLAN      2       10e7.c6d5.7119
_ipps._tcp.local                           4500     WLAN      2       10e7.c6d5.7119
_universal._sub._ipps._tcp.local           4500     WLAN      2       10e7.c6d5.7119
HP DeskJet 5000 series [D57119] (3127)._ipps._tcp.
_print._sub._ipps._tcp.local               4500     WLAN      2       10e7.c6d5.7119
HP DeskJet 5000 series [D57119] (3127)._ipps._tcp.
_ePCL._sub._ipps._tcp.local                4500     WLAN      2       10e7.c6d5.7119
HP DeskJet 5000 series [D57119] (3127)._ipps._tcp.
_ipps._tcp.local                           4500     WLAN      2       10e7.c6d5.7119
HP DeskJet 5000 series [D57119] (3127)._ipps._tcp.
_services._dns-sd._udp.local               4500     WLAN      2       10e7.c6d5.7119
_ipp._tcp.local                             4500     WLAN      2       10e7.c6d5.7119
_universal._sub._ipp._tcp.local             4500     WLAN      2       10e7.c6d5.7119
HP DeskJet 5000 series [D57119] (3127)._ipp._tcp.l
_print._sub._ipp._tcp.local                 4500     WLAN      2       10e7.c6d5.7119
HP DeskJet 5000 series [D57119] (3127)._ipp._tcp.l
_ePCL._sub._ipp._tcp.local                  4500     WLAN      2       10e7.c6d5.7119
HP DeskJet 5000 series [D57119] (3127)._ipp._tcp.l
.
.
.
----- SRV Records -----
-----
RECORD-NAME                                TTL      TYPE      ID      CLIENT-MAC
-----

```

RR-RECORD-DATA

| | | | | | |
|---|------|------|---|----------------|---|
| HP DeskJet 5000 series [D57119] (3127)._ipp._ | 4500 | WLAN | 2 | 10e7.c6d5.7119 | 0 |
| 0 631 HP10E7C6D57119-2860.local | | | | | |
| HP DeskJet 5000 series [D57119] (3127)._http. | 4500 | WLAN | 2 | 10e7.c6d5.7119 | 0 |
| 0 80 HP10E7C6D57119-2860.local | | | | | |
| HP DeskJet 5000 series [D57119] (3127)._ipps. | 4500 | WLAN | 2 | 10e7.c6d5.7119 | 0 |
| 0 631 HP10E7C6D57119-2860.local | | | | | |
| HP DeskJet 5000 series [D57119] (3127)._uscan | 4500 | WLAN | 2 | 10e7.c6d5.7119 | 0 |
| 0 8080 HP10E7C6D57119-2860.local | | | | | |
| HP DeskJet 5000 series [D57119] (3127)._prive | 4500 | WLAN | 2 | 10e7.c6d5.7119 | 0 |
| 0 80 HP10E7C6D57119-2860.local | | | | | |
| HP DeskJet 5000 series [D57119] (3127)._uscan | 4500 | WLAN | 2 | 10e7.c6d5.7119 | 0 |
| 0 443 HP10E7C6D57119-2860.local | | | | | |
| HP DeskJet 5000 series [D57119] (3127)._scann | 4500 | WLAN | 2 | 10e7.c6d5.7119 | 0 |
| 0 8080 HP10E7C6D57119-2860.local | | | | | |
| HP DeskJet 5000 series [D57119] (3127)._pdl-d | 4500 | WLAN | 2 | 10e7.c6d5.7119 | 0 |
| 0 9100 HP10E7C6D57119-2860.local | | | | | |

----- A/AAAA Records

| RECORD-NAME | TTL | TYPE | ID | CLIENT-MAC |
|---------------------------|------|------|----|----------------|
| RR-RECORD-DATA | | | | |
| HP10E7C6D57119-2860.local | 4500 | WLAN | 2 | 10e7.c6d5.7119 |
| 8.16.16.99 | | | | |

----- TXT Records

| RECORD-NAME | TTL | TYPE | ID | CLIENT-MAC |
|---|------|------|----|----------------|
| RR-RECORD-DATA | | | | |
| HP DeskJet 5000 series [D57119] (3127)._ipp._ | 4500 | WLAN | 2 | 10e7.c6d5.7119 |
| [502]'txtvers=1'adminurl=http://HP10E7C6D57119-28 | | | | |
| HP DeskJet 5000 series [D57119] (3127)._http. | 4500 | WLAN | 2 | 10e7.c6d5.7119 |
| [1]'' | | | | |
| HP DeskJet 5000 series [D57119] (3127)._ipps. | 4500 | WLAN | 2 | 10e7.c6d5.7119 |
| [502]'txtvers=1'adminurl=http://HP10E7C6D57119-28 | | | | |
| HP DeskJet 5000 series [D57119] (3127)._uscan | 4500 | WLAN | 2 | 10e7.c6d5.7119 |
| [280]'txtvers=1'adminurl=http://HP10E7C6D57119-28 | | | | |
| HP DeskJet 5000 series [D57119] (3127)._prive | 4500 | WLAN | 2 | 10e7.c6d5.7119 |
| [124]'txtvers=1'ty=HP DeskJet 5000 series [D57119 | | | | |
| HP DeskJet 5000 series [D57119] (3127)._uscan | 4500 | WLAN | 2 | 10e7.c6d5.7119 |
| [280]'txtvers=1'adminurl=http://HP10E7C6D57119-28 | | | | |
| HP DeskJet 5000 series [D57119] (3127)._scann | 4500 | WLAN | 2 | 10e7.c6d5.7119 |
| [177]'txtvers=1'adminurl=http://HP10E7C6D57119-28 | | | | |
| HP DeskJet 5000 series [D57119] (3127)._pdl-d | 4500 | WLAN | 2 | 10e7.c6d5.7119 |
| [211]'txtvers=1'rp='priority=40'UUID=9fe36149-9 | | | | |

show mdns-sd cache upn detail

To view the multicast DNS (mDNS) cache user personal network identifier details, use the **show mdns-sd cache upn detail** command.

show mdns-sd cache upn *upn-id* detail

| Syntax Description | <i>upn-id</i> User personal network identifier. | | | | |
|--------------------------------|--|---------|--------------|--------------------------------|------------------------------|
| Command Default | None | | | | |
| Command Modes | Privileged EXEC (#) | | | | |
| Command History | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Amsterdam 17.1.1s</td> <td>This command was introduced.</td> </tr> </tbody> </table> | Release | Modification | Cisco IOS XE Amsterdam 17.1.1s | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE Amsterdam 17.1.1s | This command was introduced. | | | | |

Example

The following is sample output from the **show mdns-sd cache upn detail** command that displays the mDNS cache UPN identifier details:

```
Device# show mdns-sd cache upn 777 detail
```

```
Name: _services._dns-sd._udp.local
Type: PTR
TTL: 4500
WLAN: 2
WLAN Name: mdns-psk
VLAN: 16
Client MAC: f4f9.51e2.a6a6
AP Ethernet MAC: 002a.1087.d68a
Remaining-Time: 4486
Site-Tag: default-site-tag
mDNS Service Policy: madhu-mDNS-Policy
Overriding mDNS Service Policy: NO
UPN-ID: 7777
UPN-Status: Enabled
Rdata: _airplay._tcp.local
```


show mdns-sd flexconnect summary

To view the summary of the mDNS flexconnect sites, use the **show mdns-sd flexconnect summary** command.

show mdns-sd flexconnect summary

| | | |
|---------------------------|--|------------------------------|
| Syntax Description | This command has no keywords or arguments. | |
| Command Default | None | |
| Command Modes | Privileged EXEC mode | |
| Command History | Release | Modification |
| | Cisco IOS XE Amsterdam 17.3.1 | This command was introduced. |
| Usage Guidelines | None | |

Example

The following example shows how to view the summary of mDNS flexconnect sites:

```
Device# show mdns-sd flexconnect summary
```

show mdns-sd statistics

To view the mDNS statistics, use the **show mdns-sd statistics** command.

```
show mdns-sd statistics { debug | flexconnect | rlan-id <1 - 128> wired | wlan-id <1 - 4096>
}
```

| Syntax Description | | |
|---------------------------|--|---|
| debug | | Specifies the mDNS debug statistics. |
| flexconnect | | Specifies the mDNS flexconnect statistics. |
| rlan-id <1 - 128> | | Specifies the remote LAN (RLAN) ID. The value range is from 1 to 128. |
| wired | | Specifies the mDNS wired statistics. |
| wlan-id <1 - 4096> | | Specifies the WLAN ID. The value range is from 1 to 4096. |

Command Default None

Command Modes Privileged EXEC mode

| Command History | Release | Modification |
|-----------------|-------------------------------|------------------------------|
| | Cisco IOS XE Amsterdam 17.3.1 | This command was introduced. |

Usage Guidelines None

Example

The following example shows how to view the mDNS statistics:

```
Device# show mdns-sd statistics
```

show mdns-sd summary

To view the summary of mDNS service discovery configuration, use the **show mdns-sd summary** command.

```
show mdns-sd summary
```

| | | |
|---------------------------|--|------------------------------|
| Syntax Description | This command has no keywords or arguments. | |
| Command Default | None | |
| Command Modes | Privileged EXEC mode | |
| Command History | Release | Modification |
| | Cisco IOS XE Amsterdam 17.3.1 | This command was introduced. |
| Usage Guidelines | None | |

Example

The following example shows how to view the summary of mDNS service discovery configuration:

```
Device# show mdns-sd summary
```

show mdns-sd sp-sdg statistics

To verify the Service-Peer SDG communication statistics, use the **show mdns-sd sp-sdg statistics** command.

show mdns-sd sp-sdg statistics

| | | |
|---------------------------|--|------------------------------|
| Syntax Description | This command has no keywords or arguments. | |
| Command Default | None | |
| Command Modes | Privileged EXEC | |
| Command History | Release | Modification |
| | Cisco IOS XE Bengaluru 17.5.1 | This command was introduced. |

The following example shows how to verify the Service-Peer SDG communication statistics:

```
Device# show mdns-sd sp-sdg statistics
                                One min, 5 mins, 1 hour
Average Input rate (pps) :    0,          0,          0
Average Output rate (pps) :    0,          0,          0
Messages sent:
Query : 0
ANY query : 0
Advertisements : 0
Advertisement Withdraw : 0
Interface down : 0
Vlan down : 0
Service-peer ID change : 0
Service-peer cache clear : 0
Resync response : 0
Keep-Alive : 1
Messages received:
Query response : 0
ANY Query response : 0
Cache-sync : 0
Get service-instance : 0
Keep-Alive response : 1
```

show mobility

To display information about the Layer 3 mobility and the wireless network, use the **show mobility** command in privileged EXEC mode.

```
show mobility {ap [ip-address]|mn [ip ip-address]|mac mac-address|network network-id|status}
```

| Syntax Description | Parameter | Description |
|--------------------|----------------------------------|---|
| | ap | Displays information about the access point. |
| | <i>ip-address</i> | (Optional) IP address. |
| | mn | Displays information about the mobile node. |
| | ip <i>ip-address</i> | (Optional) Displays information about the IP database thread. |
| | mac <i>mac-address</i> | Displays information about the MAC database thread. |
| | network <i>network-id</i> | Displays information for a specific wireless network ID. |
| | status | Displays status information. |

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|--------------|--|
| | 12.2(18)SXD | This command was introduced on the Supervisor Engine 720. |
| | 12.2(18)SXD3 | The output of this command was changed to include the TCP adjust-mss status. |
| | 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

Usage Guidelines This command is supported on Cisco 7600 series routers that are configured with a WLSM only.

Examples

This example shows how to display information about the access point:

```
Router# show mobility
  ap
AP IP Address   AP Mac Address Wireless Network-ID
-----
10.1.1.2 000d.29a2.a852 101 102 109 103
```

This example shows how to display information about the access points for a specific network ID:

```
Router# show mobility
  ap 172.16.1.2 detail
IP Address : 172.16.1.2
MAC Address : 000d.29a2.a852
Participating Wireless Tunnels: 101, 102, 109, 103
Registered Mobile Nodes on AP {172.16.1.2, 000d.29a2.a852} :
MN Mac Address MN IP Address AP IP Address Wireless Network-ID
-----
000a.8afa.85c9 10.1.3.11 172.16.1.2 103
```

```

000d.bdb7.83f7 10.1.2.11 172.16.1.2 102
000d.bdb7.83fb 10.1.1.11 172.16.1.2 101
Router# show mobility
  network-id 101
Wireless Network ID : 101
Wireless Tunnel Source IP Address : 10.1.1.1
Wireless Network Properties : Trusted
Wireless Network State : Up
Registered Access Point on Wireless Network 101:
AP IP Address AP Mac Address Wireless Network-ID
-----
176.16.1.2 000d.29a2.a852 101 102 109 103
Registered Mobile Nodes on Wireless Network 101:
MN Mac Address MN IP Address AP IP Address Wireless Network-ID
-----
000d.bdb7.83fb 10.1.1.11 176.16.1.2 101
Router# show mobility
  status
WLAN Module is located in Slot: 4 (HSRP State: Active) LCP
Communication status      : up
MAC address used for Proxy ARP: 0030.a349.d800
Number of Wireless Tunnels   : 1
Number of Access Points     : 2
Number of Mobile Nodes      : 0
Wireless Tunnel Bindings:
Src IP Address   Wireless Network-ID   Flags
-----
10.1.1.1        101                                   B
Flags: T=Trusted, B=IP Broadcast enabled, A=TCP Adjust-mss enabled

```

Related Commands

| Command | Description |
|-----------------|---------------------------------------|
| mobility | Configures the wireless mGRE tunnels. |

show monitor capture

To display the contents of a monitor capture buffer or a capture point, use the **show monitor capture** command in privileged EXEC mode.

```
show monitor capture [ epc-capture-name [ parameter | buffer [{ brief | detailed | dump } ] ] ]
```

| Syntax Description | |
|-------------------------|--|
| <i>epc-capture-name</i> | Specifies the name of the embedded packet capture. |
| buffer | Displays the contents of the specified capture buffer. |
| dump | (Optional) Displays a hexadecimal dump of the captured packet in addition to the metadata. |
| brief | (Optional) Provides a brief output of the captured packet information. |
| detail | (Optional) Provides a detailed output of the captured packet information. |
| parameter | Reconstructs and displays EXEC commands that were used to specify the capture. |
| detailed | Provides a detailed output of the captured packet information. |

Command Modes Privileged EXEC (#)

Command History

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

Usage Guidelines

You can enter the **show monitor capture** command when the capture buffer is not in the running state.

If you enter the **detail** keyword, packets are decoded to the Layer 4 protocol level and displayed. If you enter the **dump** keyword, non-IP packets are displayed in hexadecimal dump format. An ACL can be configured as a display filter so that only packets permitted by the ACL are displayed.

The following example shows how to display all the packets in a capture buffer. The output is self-explanatory.

```
Device# show monitor capture mycap buffer
```

```
buffer size (KB) : 2048000
buffer used (KB) : 128
packets in buf : 17
packets dropped : 0
packets per sec : 3
```

The following example shows how to display the list of commands that were used to specify the capture:

```
Device# show monitor capture cap1 parameter
```

```
monitor capture cap1 interface GigabitEthernet 1/0/1 both
```

```
monitor capture cap1 match any
monitor capture cap1 buffer size 10
monitor capture cap1 limit pps 1000
```

The following example shows how to display brief output from the captured packet information. The output is self-explanatory.

```
Device# show monitor capture cap1 buffer brief
```

```
-----
#   size  timestamp      source                destination  protocol
-----
 0   62    0.000000    10.0.0.1             -> 203.0.113.254  UDP
 1   46    0.267992    10.0.1.2             -> 203.0.113.204  IGMP
 2   76    0.428979    172.16.255.3         -> 172.16.255.3   UDP
 3   62    1.613982    10.0.29.1            -> 172.16.200.2   UDP
 4   74    1.659970    10.0.1.3             -> 10.0.0.10      EIGRP
 5   90    2.016006    10.29.0.4            -> 203.0.113.224  UDP
 6   74    2.088008    10.1.9.2             -> 203.0.113.10   EIGRP
 7   76    2.114008    172.17.254.1         -> 172.16.255.1   UDP
 8   74    2.245990    10.29.0.3            -> 203.0.113.10   EIGRP
 9   46    2.262987    10.0.0.0             -> 203.0.113.1    IGMP
10   77    2.362988    10.1.9.2             -> 203.0.113.10   EIGRP
11   62    2.631971    10.29.0.2            -> 203.0.113.2    UDP
12   74    2.934009    10.29.0.5            -> 203.0.113.10   EIGRP
13   74    3.331984    10.29.0.6            -> 203.0.113.10   EIGRP
14   46    3.499974    10.0.0.0             -> 203.0.113.1    IGMP
15   46    4.304992    10.0.0.0             -> 203.0.113.1    IGMP
16   76    5.157005    172.16.255.3         -> 172.17.255.3   UDP
```

The following example shows how to display all the packets in a capture buffer. The output is self-explanatory.

```
Device# show monitor capture cap1 buffer detailed
```

```
-----
#   size  timestamp      source                destination  protocol
-----
 0   62    0.000000    10.29.0.2             -> 172.16.255.3   UDP
0000: 01005E00 00020000 0C07AC1D 080045C0  ..^.....E.
0010: 00300000 00000111 CFDC091D 0002E000  .0.....
0020: 000207C1 07C1001C 802A0000 10030AFA  .....*.....
0030: 1D006369 73636F00 0000091D 0001      ..example.....

 1   46    0.267992    10.0.0.0             -> 172.16.255.1   IGMP
0000: 01005E00 0002001B 2BF69280 080046C0  ..^.....+.....F.
0010: 00200000 00000102 44170000 0000E000  . .....D.....
0020: 00019404 00001700 E8FF0000 0000      ..example.....

 2   76    0.428979    172.16.255.3         -> 172.17.255.3   UDP
0000: 00000C07 AC1DB414 89031124 080045C0  .....$.E.
0010: 003E0000 0000FF11 64C5AC10 FF03AC11  .>.....d.....
0020: FF030286 0286002A 84A40001 001EAC10  .....*.....
0030: FF030000 01000014 00000000 04000004  ..example.....

 3   62    1.613982    10.26.11.3           -> 172.16.255.1   UDP
0000: 01005E00 0002001B 2BF68680 080045C0  ..^.....+.....E.
0010: 00300000 00000111 CFDB091D 0003E000  .0.....
0020: 000207C1 07C1001C 88B50000 08030A6E  .....n.....
0030: 1D006369 73636F00 0000091D 0001      ..example.....

 4   74    1.659970    10.29.3.2            -> 172.16.255.2   EIGRP
0000: 01005E00 000A001B 2BF69280 080045C0  ..^.....+.....E.
```



```

0010: 003C0000 00000258 CE81091D 0002E000  .<.....X.....
0020: 000A0205 F3000000 00000000 00000000  .....
0030: 00000000 00D10001 000C0100 01000000  .....

  5  90    2.016006  10.22.1.4      -> 203.0.113.1    UDP
0000: FFFFFFFF FFFF001C 0F2EDC00 080045C0  .....E.
0010: 004C0000 00000111 AFC1091D 0004FFFF  .L.....
0020: FFFF007B 007B0038 5B14E500 06E80000  ...{.8[.....
0030: 00000021 BE23494E 49540000 00000000  ...!.#INIT.....

```

The following example shows how to display a hexadecimal dump of the captured packet:

```

Device# show monitor capture cap1 buffer dump
0
0000: 01005E00 00020000 0C07AC1D 080045C0  ..^.....E.
0010: 00300000 00000111 CFDC091D 0002E000  .0.....
0020: 000207C1 07C1001C 802A0000 10030AFA  .....*.....
0030: 1D006369 73636F00 0000091D 0001      ..example.....

1
0000: 01005E00 0002001B 2BF69280 080046C0  ..^.....+.....F.
0010: 00200000 00000102 44170000 0000E000  . .....D.....
0020: 00019404 00001700 E8FF0000 0000      .....

2
0000: 01005E00 0002001B 2BF68680 080045C0  ..^.....+.....E.
0010: 00300000 00000111 CFDB091D 0003E000  .0.....
0020: 000207C1 07C1001C 88B50000 08030A6E  .....n.....
0030: 1D006369 73636F00 0000091D 0001      ..example.....

3
0000: 01005E00 000A001C 0F2EDC00 080045C0  ..^.....E.
0010: 003C0000 00000258 CE7F091D 0004E000  .<.....X.....
0020: 000A0205 F3000000 00000000 00000000  .....
0030: 00000000 00D10001 000C0100 01000000  .....
0040: 000F0004 00080501 0300      .....

```

show nmosp

To display the Network Mobility Services Protocol (NMSP) configuration settings, use the **show nmosp** command.

```
show nmosp {attachment | {suppress interfaces} | capability | notification interval | statistics
{connection | summary} | status | subscription detail [ip-addr ] | summary}
```

| Syntax Description | | |
|---------------------------------------|--|---|
| attachment suppress interfaces | | Displays attachment suppress interfaces. |
| capability | | Displays NMSP capabilities. |
| notification interval | | Displays the NMSP notification interval. |
| statistics connection | | Displays all connection-specific counters. |
| statistics summary | | Displays the NMSP counters. |
| status | | Displays status of active NMSP connections. |
| subscription detail ip-addr | | The details are only for the NMSP services subscribed to by a specific IP address. |
| subscription summary | | Displays details for all of the NMSP services to which the controller is subscribed. The details are only for the NMSP services subscribed to by a specific IP address. |

Command Default No default behavior or values.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

The following is sample output from the **show nmosp notification interval** command:

```
Device# show nmosp notification interval
NMSP Notification Intervals
-----

RSSI Interval:
  Client           : 2 sec
  RFID             : 2 sec
  Rogue AP         : 2 sec
  Rogue Client     : 2 sec
Attachment Interval : 30 sec
Location Interval  : 30 sec
```

show nmsp cloud-services statistics

To see NMSP cloud-service statistics, use the **show nmsp cloud-services statistics** command.

```
show nmsp cloud-services statistics [chassis {chassis-number | active | standby} R0]
```

Syntax Description

chassis-number Chassis number as either 1 or 2.

active R0 Active instance of the active NMSP cloud services in Route-processor slot 0.

standby R0 Standby instance of the active NMSP cloud services in Route-processor slot 0.

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Examples

This example shows how to see NMSP cloud-service statistics:

```
Device# show nmsp cloud-services statistics
```

show nmosp cloud-services summary

To see a summary of information about NMSP cloud-services, use the **show nmosp cloud-services summary** command.

show nmosp cloud-services summary [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

| Syntax Description | <i>chassis-number</i> Chassis number as either 1 or 2. | | | | |
|--------------------------------|---|---------|--------------|--------------------------------|---|
| active R0 | Active instance of the NMSP cloud services in Route-processor slot 0. | | | | |
| standby R0 | Standby instance of the active NMSP cloud services in Route-processor slot 0. | | | | |
| Command Default | None | | | | |
| Command Modes | Privileged EXEC | | | | |
| Command History | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.10.1</td> <td>This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td> </tr> </tbody> </table> | 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. |
| 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

This example shows how to see NMSP cloud-service summary information:

```
Device# show nmosp cloud-services summary
```

show nmsp subscription group detail all

To display the mobility services group subscription details of all CMX connections, use the **show nmsp subscription group detail all** command.

show nmsp subscription group detail all

| Syntax Description | This command has no keywords or arguments. | | | | |
|--------------------------------|--|---------|--------------|--------------------------------|------------------------------|
| Command Default | None | | | | |
| Command Modes | Privileged EXEC (#) | | | | |
| Command History | <table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>Cisco IOS XE Gibraltar 16.10.1</td><td>This command was introduced.</td></tr></tbody></table> | Release | Modification | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. | | | | |

Example

The following example shows how to display the mobility services group subscription details of all CMX connections:

```
Device# show nmsp subscription group detail all
```

show nmsp subscription group detail ap-list

To display the AP MAC list subscribed for a group by a CMX connection, use the **show nmsp subscription group detail ap-list** command.

show nmsp subscription group detail ap-list *group-name cmx-IP-address*

| | | |
|---------------------------|--------------------------------|------------------------------|
| Syntax Description | <i>group-name</i> | CMX AP group name. |
| | <i>cmx-IP-address</i> | CMX IP address. |
| Command Default | None | |
| Command Modes | Privileged EXEC (#) | |
| Command History | Release | Modification |
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

Example

The following example shows how to verify the AP MAC list subscribed for a group by a CMX connection.

```
Device# show nmsp subscription group detail ap-list Group1 127.0.0.1

CMX IP address: 127.0.0.1
CMX Group name: Group1
CMX Group AP MACs:
: 00:00:00:00:70:02 00:00:00:00:66:02 00:99:00:00:00:02 00:00:00:bb:00:02
  00:00:00:00:55:02 00:00:00:00:50:02 00:33:00:00:00:02 00:d0:00:00:00:02
  00:10:00:10:00:02 00:00:00:06:00:02 00:00:00:02:00:02 00:00:00:00:40:02
  00:00:00:99:00:02 00:00:00:00:a0:02 00:00:77:00:00:02 00:22:00:00:00:02
  00:00:00:00:00:92 00:00:00:00:00:82 00:00:00:00:03:02 aa:00:00:00:00:02
  00:00:00:50:00:42 00:00:0d:00:00:02 00:00:00:00:00:32 00:00:00:cc:00:02
  00:00:00:88:00:02 20:00:00:00:00:02 10:00:00:00:00:02 01:00:00:00:00:02
  00:00:00:00:00:02 00:00:00:00:00:01 00:00:00:00:00:00
```

show nmsp subscription group detail services

To display the services subscribed for a group by a CMX connection, use the **show nmsp subscription group detail services** command.

show nmsp subscription group detail services *group-name cmx-IP-address*

Syntax Description

| | |
|-----------------------|--------------------|
| <i>group-name</i> | CMX AP group name. |
| <i>cmx-IP-address</i> | CMX IP address. |

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

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

Example

The following example shows how to verify the services subscribed for a group by a CMX connection.

```
Device# show nmsp subscription group detail services Group1 127.0.0.1

CMX IP address: 127.0.0.1
CMX Group name: Group1
CMX Group filtered services:
Service          Subservice
-----
RSSI              Mobile Station,
Spectrum
Info
Statistics
```

show nmsp subscription group summary

To display the mobility services group subscription summary of all CMX connections, use the **show nmsp subscription group summary** command.

show nmsp subscription group summary

| | | |
|---------------------------|--|------------------------------|
| 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. |

Example

The following example shows how to verify the mobility services group subscription summary of all CMX connections.

```
Device# show nmsp subscription group summary
CMX IP address: 127.0.0.1
Groups subscribed by this CMX server:
Group name: Group1
```


show ntp associations

To display the status of Network Time Protocol (NTP) associations, use the **show ntp associations** command in privileged EXEC mode.

show ntp associations

| | |
|---------------------------|--|
| Syntax Description | This command has no keywords or arguments. |
|---------------------------|--|

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

| | |
|----------------------|--------------------|
| Command Modes | Privileged EXEC(#) |
|----------------------|--------------------|

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

Example

The following example shows how to view NTP associations. :

```
Device# show ntp associations
  address      ref clock      st  when  poll reach  delay  offset  disp
*~10.1.1.99    72.163.32.44  2   918   1024  377  0.177  7.618  1.102
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
--
```

show parameter-map type webauth name

To verify the webauth parameters of a parameter map, use the **show parameter-map type webauth name** command.

show parameter-map type webauth name *parameter-map name*

| | |
|---------------------------|--|
| Syntax Description | <i>parameter-map name</i> Name of the parameter map. |
|---------------------------|--|

| | |
|------------------------|------|
| 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 verify the webauth parameters of a parameter map:

```
Device# configure terminal
Device(config)# show parameter-map type webauth name parameter-map-name
```

show platform conditions

To see information about conditional debugs, use the **show platform conditions** command.

show platform conditions

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Examples

The following example shows how to see information about conditional debugs:

```
Device# show platform conditions
```

show platform hardware

To see the hardware platform Quantum flow processor datapath statistics, use the **show platform hardware chassis active qfp feature wireless wlclient datapath cpp-if-handle statistics** command.

show hardware chassis active qfp feature wireless wlclient datapath cpp-if-handle *client-cpp-value* **statistics** {**clear** | **start** | **stop**}

| Syntax Description | active | Active instance. |
|--------------------|--------------------------------|---|
| | qfp | Quantum Flow Processor. |
| | wlclient | QFP wireless client. |
| | cpp-if-handle | client cpp interface handle. |
| | <i>client-cpp-value</i> | Client cpp if-handle value. The range is between 1 and 4294967295. |
| | statistics | Show Client Statistics. |
| | clear | Shows and Clears the Client Statistics. |
| | start | Start Client Statistics collection. |
| | stop | Stop Client Statistics collection. |
| Command Default | None | |
| Command Modes | Privileged EXEC | |
| Command History | Release | Modification |
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

Examples

The following example shows how to start client statistics collection:

```
Device# show platform hardware chassis active qfp feature wireless wlclient datapath
cpp-if-handle cpp-if-handle value statistics start
```

show platform hardware chassis active qfp feature dns-snoop-agent client enabled-intf

To view the DSA enabled interfaces, use the **show platform hardware chassis active qfp feature dns-snoop-agent client enabled-intf** command.

```
show platform hardware chassis active qfp feature dns-snoop-agent client enabled-intf
```

| | | |
|---------------------------|--------------------------------|------------------------------|
| Syntax Description | This command has no arguments. | |
| Command Default | None | |
| Command Modes | Global configuration | |
| Command History | Release | Modification |
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the DSA enabled interfaces:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent client enabled-intf
Interface name: GigabitEthernet0/0/0, handle: 5
```

show platform hardware chassis active qfp feature dns-snoop-agent client hw-pattern-list

To view the OpenDNS string or FQDN filter for the pattern list, use the **show platform hardware chassis active qfp feature dns-snoop-agent client hw-pattern-list** command.

```
show platform hardware chassis active qfp feature dns-snoop-agent client hw-pattern-list
{fqdn-filter fqdn_filter_ID | odns_string}
```

| | |
|---------------------------|--|
| Syntax Description | fqdn-filter Displays the FQDN filter for the pattern list. |
| | <i>fqdn_filter_ID</i> Refers to the FQDN filter ID. The valid range is from 1 to 16. |
| | odns_string Displays the OpenDNS string for the pattern list. |

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

| | |
|----------------------|----------------------|
| Command Modes | Global configuration |
|----------------------|----------------------|

| | | |
|------------------------|--------------------------------|------------------------------|
| Command History | Release | Modification |
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the FQDN filter for the pattern list:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent client
hw-pattern-list fqdn-filter 1
Filter Name: url1list_flex_preauth

Name: url1.dns.com
Feature mask: 16, Dirty: 0, Ref count: 0, Match count: 0
```

show platform hardware chassis active qfp feature dns-snoop-agent client info

To view the DSA client details, use the **show platform hardware chassis active qfp feature dns-snoop-agent client info** command.

show platform hardware chassis active qfp feature dns-snoop-agent client info

Syntax Description

This command has no arguments.

Command Default

None

Command Modes

Global configuration

Command History

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

This example shows how to view the DSA client details:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent client info
Number of patterns added/deleted/total: 2/0/2
Number of re_table rebuilt : : 0
Number of str_table rebuilt: : 2
Registered clients: 0x001ffff0
Number of transaction started/ended: 2/2
Memory pool size/limit: 512/81920
Pending Deletion Pattern List:
```

show platform hardware chassis active qfp feature dns-snoop-agent client pattern-list

To view the OpenDNS string or FQDN filter for the pattern list, use the **show platform hardware chassis active qfp feature dns-snoop-agent client pattern-list** command.

```
show platform hardware chassis active qfp feature dns-snoop-agent client pattern-list {fqdn-filter
fqdn_filter_ID | odns_string}
```

| | |
|---------------------------|--|
| Syntax Description | fqdn-filter Displays the FQDN filter for the pattern list. |
| | fqdn_filter_ID Refers to the FQDN filter ID. The valid range is from 1 to 16. |
| | odns_string Displays the OpenDNS string for the pattern list. |

Command Default None

Command Modes Global configuration

| Command History | Release | Modification |
|------------------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the FQDN filter for the pattern list:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent client pattern-list
fqdn-filter 1
Filter Name: url1list_flex_preauth
Pattern List in CPP client: 1

Name: url1.dns.com
feature_mask: 0x00000010, hw_ptr: 0xdf86d510
```


show platform hardware chassis active qfp feature dns-snoop-agent datapath ip-cache

To view the DSA IP cache table details, use the **show platform hardware chassis active qfp feature dns-snoop-agent datapath ip-cache** command.

```
show platform hardware chassis active qfp feature dns-snoop-agent datapath ip-cache {address
[ipv4 ipv4_address | ipv6 ipv6_address] | all | pattern regex_pattern}
```

| Syntax Description | address [ipv4 ipv4_address ipv6 ipv6_address] | Displays the DSA address entry details |
|--------------------|---|---|
| | all | Displays all the DSA IP cache address details |
| | pattern <i>regex_pattern</i> | Displays the DSA IP cache pattern details |

Command Default None

Command Modes Global configuration

| Command History | Release | Modification |
|-----------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the DSA address entry details:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent datapath ip-cache
address ipv4 104.122.2.194
IP address: 104.122.2.194, client(s): 32, regex: www.adobe.com, expire in 0 seconds
```

This example shows how to view all the DSA IP cache address details:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent datapath ip-cache
all
IP Address          Client(s)  Expire    Match          RegexId      Dirty
-----
172.217.13.228     2          132      .*google.com   0x4d7f9e20   0x0
```

This example shows how to view the DSA IP cache pattern details:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent datapath ip-cache
pattern .*google*
1 IP Addresses matching pattern .*google*
IP Address          Client(s)  Expire    Match          RegexId      Dirty
-----
2607:f8b0:4004:800:0:0:2004  32         13       .*google*     0x31156220   0x0
```

show platform hardware chassis active qfp feature dns-snoop-agent datapath memory

To view the DSA datapath memory details, use the **show platform hardware chassis active qfp feature dns-snoop-agent datapath memory** command.

show platform hardware chassis active qfp feature dns-snoop-agent datapath memory

| | | |
|---------------------------|--------------------------------|------------------------------|
| Syntax Description | This command has no arguments. | |
| Command Default | None | |
| Command Modes | Global configuration | |
| Command History | Release | Modification |
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the DSA datapath memory details:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent datapath memory
Table-Name  Address      Size
-----
IP Cache DB  0xda5bb420  512
IP Hash      0xda41f400  1024
String Table 0xdec6ac10
String Table 0xda41f010

==DSA Chunk info==
Chunk-Pool  Allocated    Total_Free  Init-Num    Low_Wat
-----
ip cache chunk  0              512          512          512

==DSA Runtime Info==
-----
dsa init state 0x7   dsa client mask 0x100010
```

show platform hardware chassis active qfp feature dns-snoop-agent datapath regexp-table

To view the DSA regular expression table, use the **show platform hardware chassis active qfp feature dns-snoop-agent datapath regexp-table** command.

```
show platform hardware chassis active qfp feature dns-snoop-agent datapath regexp-table
```

| | | |
|---------------------------|--------------------------------|------------------------------|
| Syntax Description | This command has no arguments. | |
| Command Default | None | |
| Command Modes | Global configuration | |
| Command History | Release | Modification |
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the DSA regular expression table:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent datapath
regexp-table
String Table 0xdec6ac10      WLS_FQDN_GRP_1
String Table 0xda41f010      ODNS String
```

show platform hardware chassis active qfp feature dns-snoop-agent datapath stats

To view the DSA statistics, use the **show platform hardware chassis active qfp feature dns-snoop-agent datapath stats** command.

show platform hardware chassis active qfp feature dns-snoop-agent datapath stats

| | | |
|---------------------------|--------------------------------|------------------------------|
| Syntax Description | This command has no arguments. | |
| Command Default | None | |
| Command Modes | Global configuration | |
| Command History | Release | Modification |
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the DSA statistics:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent datapath stats
DNS Snoop Agent Stats:
  parser unknown pkt: 0
  parser not needed: 0
  parser fmt error: 0
  parser pa error: 0
  parser non resp: 0
  parser multiple name: 0
  parser dns name err: 0
  parser matched ip: 0
  parser redirect: 0
  parser whitelist redirect: 0
  parser blacklist redirect: 0
  parser invalid redirect ip: 0
  parser skip: 0
  regex locked: 0
  regex not matched: 0
  pkt drop whitelist no redirect ip: 0
  pkt drop blacklist no redirect ip: 0
  entries in use: 0
  ip cache allocation fail: 0
  ip addr add: 0
  ip addr update: 0
  ip addr delete: 0
  ip addr cache hit: 0
  ip addr cache miss: 0
  ip addr bad param: 0
  ip addr delete not found: 0
  ip cache not initialized: 0
```

show platform hardware chassis active qfp feature et-analytics datapath runtime

To view the ETA global state in datapath, use the **show platform hardware chassis active qfp feature et-analytics datapath runtime** command.

show platform hardware chassis active qfp feature et-analytics datapath runtime

| | |
|---------------------------|--|
| Syntax Description | This command has no keywords or arguments. |
|---------------------------|--|

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

| | |
|----------------------|----------------------|
| Command Modes | Global configuration |
|----------------------|----------------------|

| Command History | Release | Modification |
|------------------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.11.1 | This command was introduced. |

This example shows how to view the ETA global and interface details:

```
Device# show platform hardware chassis active qfp feature et-analytics datapath runtime
ET-Analytics run-time information:
  Feature state: initialized (0x00000004)
  Inactive timeout : 15 secs (default 15 secs)
  WhiteList information :
    flag: False
    cgacl w0 : n/a
    cgacl w1 : n/a
  Flow CFG information :
    instance ID : 0x0
    feature ID : 0x1
    feature object ID : 0x1
    chunk ID : 0xC
```

show platform hardware chassis active qfp feature et-analytics datapath memory

To view the ETA memory details, use the **show platform hardware chassis active qfp feature et-analytics datapath memory** command.

show platform hardware chassis active qfp feature et-analytics datapath memory

| | | |
|---------------------------|--------------------------------|------------------------------|
| Syntax Description | This command has no arguments. | |
| Command Default | None | |
| Command Modes | Global configuration | |
| Command History | Release | Modification |
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the ETA memory details:

```
Device# show platform hardware chassis active qfp feature et-analytics datapath memory
ET-Analytics memory information:
  Size of FO : 3200 bytes
  No. of FO allocs : 0
  No. of FO frees : 0
```

show platform hardware chassis active qfp feature et-analytics datapath stats export

To view the ETA flow export in datapath, use the **show platform hardware chassis active qfp feature et-analytics datapath stats export** command.

show platform hardware chassis active qfp feature et-analytics datapath stats export

| | | |
|---------------------------|--------------------------------|------------------------------|
| Syntax Description | This command has no arguments. | |
| Command Default | None | |
| Command Modes | Global configuration | |
| Command History | Release | Modification |
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the ETA flow export in datapath:

```
Device# show platform hardware chassis active qfp feature et-analytics datapath stats export
ET-Analytics 192.168.5.2:2055 vrf 0 Stats:
  Export statistics:
    Total records exported : 5179231
    Total packets exported : 3124873
    Total bytes exported : 3783900196
    Total dropped records : 0
    Total dropped packets : 0
    Total dropped bytes : 0
    Total IDP records exported :
      initiator->responder : 1285146
      responder->initiator : 979284
    Total SPLT records exported:
      initiator->responder : 1285146
      responder->initiator : 979284
    Total SALT records exported:
      initiator->responder : 0
      responder->initiator : 0
    Total BD records exported :
      initiator->responder : 0
      responder->initiator : 0
    Total TLS records exported :
      initiator->responder : 309937
      responder->initiator : 329469
```

show platform hardware chassis active qfp feature et-analytics datapath stats flow

To view the ETA flow statistics, use the **show platform hardware chassis active qfp feature et-analytics datapath stats flow** command.

show platform hardware chassis active qfp feature et-analytics datapath stats flow

| | | |
|---------------------------|--------------------------------|------------------------------|
| Syntax Description | This command has no arguments. | |
| Command Default | None | |
| Command Modes | Global configuration | |
| Command History | Release | Modification |
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the ETA flow statistics:

```
Device# show platform hardware chassis active qfp feature et-analytics datapath stats flow
ET-Analytics Stats:
  Flow statistics:
    feature object allocs : 0
    feature object frees : 0
    flow create requests : 0
    flow create matching : 0
    flow create successful: 0
    flow create failed, CFT handle: 0
    flow create failed, getting FO: 0
    flow create failed, malloc FO : 0
    flow create failed, attach FO : 0
    flow create failed, match flow: 0
    flow create, aging already set: 0
    flow ageout requests : 0
    flow ageout failed, freeing FO: 0
    flow ipv4 ageout requests : 0
    flow ipv6 ageout requests : 0
    flow whitelist traffic match : 0
```


show platform hardware chassis active qfp feature wireless et-analytics eta-pending-client-tree

To view clients in the ETA pending wireless client tree, use the **show platform hardware chassis active qfp feature wireless et-analytics eta-pending-client-tree** command.

show platform hardware chassis active qfp feature wireless et-analytics eta-pending-client-tree

Syntax Description This command has no arguments.

Command Default None

Command Modes Global configuration

| Command History | Release | Modification |
|-----------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view clients in the ETA pending wireless client tree:

```
Device# show platform hardware chassis active qfp feature wireless et-analytics
eta-pending-client-tree
CPP IF_H      DPIDX      MAC Address  VLAN  AS  MS  WLAN      POA
-----
0X2A         0XA0000001  2c33.7a5b.827b  160   RN  LC  ewlc_ssid 0x90000003
0X2B         0XA0000002  2c33.7a5b.80fb  160   RN  LC  ewlc_ssid 0x90000003
```

show platform hardware chassis active qfp feature wireless et-analytics statistics

To view the ETA pending wireless client tree statistics, use the **show platform hardware chassis active qfp feature wireless et-analytics statistics** command.

show platform hardware chassis active qfp feature wireless et-analytics statistics

| | | |
|---------------------------|--------------------------------|------------------------------|
| Syntax Description | This command has no arguments. | |
| Command Default | None | |
| Command Modes | Global configuration | |
| Command History | Release | Modification |
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the ETA pending wireless client tree statistics:

```
Device# show platform hardware chassis active qfp feature wireless et-analytics statistics
Wireless ETA cpp-client plumbing statistics
Number of ETA pending clients : 2
Counter                                     Value
-----
Enable ETA on wireless client called         0
Delete ETA on wireless client called         0
ETA global cfg init cb TVI FIA enable error  0
ETA global cfg init cb output SB read error  0
ETA global cfg init cb output SB write error 0
ETA global cfg init cb input SB read error   0
ETA global cfg init cb input SB write error  0
ETA global cfg init cb TVI FIA enable success 0
ETA global cfg uninit cb ingress feat disable 0
ETA global cfg uninit cb ingress cfg delete  0
ETA global cfg uninit cb egress feat disable 0
ETA global cfg uninit cb egress cfg delete er 0
ETA pending list insert entry called         4
ETA pending list insert invalid arg error    0
ETA pending list insert entry exists error   0
ETA pending list insert no memory error      0
ETA pending list insert entry failed         0
ETA pending list insert entry success        4
ETA pending list delete entry called         2
ETA pending list delete invalid arg error    0
ETA pending list delete entry missing        0
ETA pending list delete entry remove error   0
ETA pending list delete entry success        2
```

show platform hardware slot R0 ha_port interface stats

To see the HA port interface setting status, use the **show platform hardware slot R0 ha_port interface stats** command.

show platform hardware slot R0 ha_port interface stats

| Syntax Description | This command has no arguments or keywords. | | | | |
|-------------------------------|---|---------|--------------|-------------------------------|------------------------------|
| Command Modes | Privileged EXEC (#) | | | | |
| Command History | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Bengaluru 17.5.1</td> <td>This command was introduced.</td> </tr> </tbody> </table> | Release | Modification | Cisco IOS XE Bengaluru 17.5.1 | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE Bengaluru 17.5.1 | This command was introduced. | | | | |

Examples

This example shows how to see the HA port interface setting status:

```
Device# show platform hardware slot R0 ha_port interface stats
HA Port
ha_port  Link encap:Ethernet  HWaddr 70:18:a7:c8:80:70
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
          Memory:e0900000-e0920000
```

```
Settings for ha_port:
Supported ports:          [ TP ]
Supported link modes:    10baseT/Half 10baseT/Full
                        100baseT/Half 100baseT/Full
                        1000baseT/Full
Supported pause frame use: Symmetric
Supports auto-negotiation: Yes
Supported FEC modes:     Not reported
Advertised link modes:   10baseT/Half 10baseT/Full
                        100baseT/Half 100baseT/Full
                        1000baseT/Full
Advertised pause frame use: Symmetric
Advertised auto-negotiation: Yes
Advertised FEC modes:   Not reported
Speed:                   Unknown!
Duplex:                   Unknown! (255)
Port:                     Twisted Pair
PHYAD:                   1
Transceiver:              internal
Auto-negotiation:        on
MDI-X:                   off (auto)
Supports Wake-on:        pumbg
Wake-on:                  g
Current message level:    0x00000007 (7)
                          drv probe link
Link detected:           no
```

show platform hardware slot R0 ha_port interface stats

```

NIC statistics:
  rx_packets:          0
  tx_packets:          0
  rx_bytes:            0
  tx_bytes:            0
  rx_broadcast:        0
  tx_broadcast:        0
  rx_multicast:        0
  tx_multicast:        0
  multicast:           0
  collisions:          0
  rx_crc_errors:       0
  rx_no_buffer_count:  0
  rx_missed_errors:    0
  tx_aborted_errors:   0
  tx_carrier_errors:   0
  tx_window_errors:    0
  tx_abort_late_coll:  0
  tx_deferred_ok:      0
  tx_single_coll_ok:   0
  tx_multi_coll_ok:    0
  tx_timeout_count:    0
  rx_long_length_errors: 0
  rx_short_length_errors: 0
  rx_align_errors:     0
  tx_tcp_seg_good:     0
  tx_tcp_seg_failed:   0
  rx_flow_control_xon: 0
  rx_flow_control_xoff: 0
  tx_flow_control_xon: 0
  tx_flow_control_xoff: 0
  rx_long_byte_count:  0
  tx_dma_out_of_sync:  0
  tx_smbus:            0
  rx_smbus:            0
  dropped_smbus:       0
  os2bmc_rx_by_bmc:    0
  os2bmc_tx_by_bmc:    0
  os2bmc_tx_by_host:   0
  os2bmc_rx_by_host:   0
  tx_hwtstamp_timeouts: 0
  rx_hwtstamp_cleared: 0
  rx_errors:           0
  tx_errors:           0
  tx_dropped:          0
  rx_length_errors:    0
  rx_over_errors:      0
  rx_frame_errors:     0
  rx_fifo_errors:      0
  tx_fifo_errors:      0
  tx_heartbeat_errors: 0
  tx_queue_0_packets:  0
  tx_queue_0_bytes:    0
  tx_queue_0_restart:  0
  tx_queue_1_packets:  0
  tx_queue_1_bytes:    0
  tx_queue_1_restart:  0
  rx_queue_0_packets:  0
  rx_queue_0_bytes:    0
  rx_queue_0_drops:    0
  rx_queue_0_csum_err: 0
  rx_queue_0_alloc_failed: 0
  rx_queue_1_packets:  0

```

```
rx_queue_1_bytes:      0
rx_queue_1_drops:      0
rx_queue_1_csum_err:   0
rx_queue_1_alloc_failed:0
```

show platform integrity

To view the checksum record for boot stages, use the **show platform integrity** command.

show platform integrity [**sign** [**nonce** *nonce*]]

| Syntax Description | sign (Optional). Show signature. | | | | |
|-------------------------------|---|---------|--------------|-------------------------------|------------------------------|
| | nonce (Optional). Enter a nonce value. | | | | |
| Command Default | None | | | | |
| Command Modes | Privileged EXEC | | | | |
| Command History | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Bengaluru 17.4.1</td> <td>This command was introduced.</td> </tr> </tbody> </table> | Release | Modification | Cisco IOS XE Bengaluru 17.4.1 | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE Bengaluru 17.4.1 | This command was introduced. | | | | |

The following example shows how to view the checksum record for boot stages:

```
Device# show platform integrity sign nonce 123
Platform: C9800-L-F-K9
Boot 0 Version: R04.1173930452019-06-11
Boot 0 Hash: A6C92C44976FC77DD42234444FFD87798FB9036A2762FAA4999A190A0258B18C
Boot Loader Version: 16.12(1r)
Boot Loader Hash:
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
OS Version: 2020-03-19_20.26
OS Hashes:
C9800-L-universalk9_wlc.2020-03-19_20.26.SSA.bin:
53E2DF1A1A082E36FA4CAB817C1794EC9D69AC0E90BCCBF99BCD0BCA9385AA9E9372AEF7431E4A08FC5E5B9670131C09D158E5B8A7B457501FE77AB9F1C26D
C9800-L-mono-universalk9_wlc.2020-03-19_20.26.SSA.pkg:
1D3279D53B0311CE42C669824DF86FB5596CD7CA45CA8D7FDC3D10657B8C9A48F4B0508D7BCFFD645CB6571AC1E674A57A82414E3D6E1666EE64E6132F707671
PCR0: EE14A2D5099DA343B3941C54A429C4AC1D3EE8E9B609F1AC00049768A470734E
PCR8: 78794D0F5667F8FA4E425E3CA2AF3CD99B90B219FD90222D622B3D563416BBAA
```

show platform software audit

To display the Security Enhanced Linux (SELinux) audit logs, use the **show platform software audit** command in privileged EXEC mode.

show platform software audit {all | summary | 0 | 1 | 2 | F0 | R0 | FP active | RP active}

| Syntax Description | |
|--------------------|---|
| all | Shows the audit log from all the slots. |
| summary | Shows the audit log summary count from all the slots. |
| 0 | Shows the audit log for the SM-Inter-Processor slot 0. |
| 1 | Shows the audit log for the SM-Inter-Processor slot 1. |
| 2 | Shows the audit log for the SM-Inter-Processor slot 2. |
| F0 | Shows the audit log for the Embedded-Service-Processor slot 0. |
| R0 | Shows the audit log for the Route-Processor slot 0. |
| FP active | Shows the audit log for the active Embedded-Service-Processor slot. |
| RP active | Shows the audit log for the active Route-Processor slot. |

Command Modes Privileged EXEC (#)

| Command History | Release | Modification |
|-----------------|--------------------------------|--|
| | Cisco IOS XE Gibraltar 16.11.1 | This command was introduced on Cisco ISR 4000 series routers, Cisco CSR 1000V series routers, and Cisco 1000 ISR series routers running time-sensitive networking (TSN). |
| | Cisco IOS XE Gibraltar 16.12.1 | This command was implemented on Cisco Catalyst 9800 Series Wireless Controller. |

Usage Guidelines The **show platform software audit** command displays the system logs containing the access violation events. In Cisco IOS XE Gibraltar 16.11.1, operation in a permissive mode is available - with the intent of confining specific components (process or application) of the IOS-XE platform. In the permissive mode, access violation events are detected and system logs are generated, but the event or operation itself is not blocked. The solution operates mainly in an access violation detection mode.

The following is a sample output of the **show software platform software audit summary** command:

```
Device# show platform software audit summary
=====
AUDIT LOG ON ACTIVE
-----
AVC Denial count: 7
```

The following is a sample output of the **show software platform software audit all** command. This command displays the information in the `audit.log` file.

```
Device# show platform software audit all
=====
AUDIT LOG ON ACTIVE
-----
===== START =====
type=DAEMON_START msg=audit(1553837190.262:3031): op=start ver=2.6.6 format=raw kernel=4.4.172
  auid=4294967295 pid=446 subj=system_u:system_r:auditd_t:s0 res=success
type=NETFILTER_CFG msg=audit(1553837185.956:2): table=nat family=2 entries=0
type=MAC_STATUS msg=audit(1553837186.523:3): enforcing=1 old_enforcing=0 auid=4294967295
ses=4294967295
type=SYSCALL msg=audit(1553837186.523:3): arch=c000003e syscall=1 success=yes exit=1 a0=3
a1=7ffcflc22070 a2=1 a3=0 items=0 ppid=203 pid=205 auid=4294967295 uid=0 gid=0 euid=0 suid=0
  fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="load_policy"
exe="/usr/sbin/load_policy" subj=kernel key=(null)
type=PROCTITLE msg=audit(1553837186.523:3):
proctitle=2F7573722F7362696E2F6C6F61645F706F6C696379002D69
type=MAC_POLICY_LOAD msg=audit(1553837186.528:4): policy loaded auid=4294967295 ses=4294967295
type=SYSCALL msg=audit(1553837186.528:4): arch=c000003e syscall=1 success=yes exit=1693637
  a0=4 a1=7f792d1d6000 a2=19d7c5 a3=f items=0 ppid=203 pid=205 auid=4294967295 uid=0 gid=0
euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="load_policy"
exe="/usr/sbin/load_policy" subj=system_u:system_r:kernel_t:s0 key=(null)
...

```

You can use the output of this command to copy the contents of `audit.log` to a file to then transfer to a remote host.

```
Device# show platform software audit all | redirect bootflash:audi_123.log

Device#dir bootflash:audi_123.log
Directory of bootflash:/audi_123.log
 27  -rw-          35305  Mar 29 2019 22:16:36 +00:00  audi_123.log

3249049600 bytes total (538112000 bytes free)

```


show platform software arp broadcast

To display the Address Resolution Protocol (ARP) broadcast status on an access point (AP), use the **show platform software arp broadcast** command.

show platform software arp broadcast

| Syntax Description | This command has no arguments or keywords. | | | | |
|-------------------------------|---|---------|--------------|-------------------------------|------------------------------|
| Command Default | None | | | | |
| Command Modes | Privileged EXEC (#) | | | | |
| Command History | <table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>Cisco IOS XE Cupertino 17.8.1</td><td>This command was introduced.</td></tr></tbody></table> | Release | Modification | Cisco IOS XE Cupertino 17.8.1 | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE Cupertino 17.8.1 | This command was introduced. | | | | |

Examples

The following example shows the ARP broadcast on an AP:

```
Device# show platform software arp broadcast
```

```
Arp broadcast is enabled on vlans:  
20,50
```

show platform software system all

To check status of the current virtual machine and look for performance issues due to inadequate resources (or other issues with the hosting environment), use the **set platform software system all** command in privileged EXEC mode.

show platform software system all

| | |
|---------------------------|--|
| Syntax Description | This command has no keywords or arguments. |
|---------------------------|--|

| | |
|----------------------|---------------------|
| Command Modes | Privileged EXEC (#) |
|----------------------|---------------------|

| | | |
|------------------------|--------------------------------|------------------------------|
| Command History | Release | Modification |
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

Examples

This example shows how to check status of the current virtual machine and its resources:

```
Device# show platform software system all

Processor Details
=====
Number of Processors : 6
Processor : 1 - 6
vendor_id : GenuineIntel
cpu MHz : 2593.750
cache size : 35840 KB
Crypto Supported : Yes
model name : Intel(R) Xeon(R) CPU E5-2690 v4 @ 2.60GHz

Memory Details
=====
Physical Memory : 16363904KB

VNIC Details
=====
Name      Mac Address  Status Platform MTU
GigabitEthernet1 000c.2964.7126  UP 1500
GigabitEthernet2 000c.2964.7130  UP 1500

Hypervisor Details
=====
Hypervisor: VMWARE
Manufacturer: VMware, Inc.
Product Name: VMware Virtual Platform
Serial Number: VMware-56 4d e5 0a a7 dd 27 2b-0e 2f 36 6e 0f 64 71 26
UUID: 564DE50A-A7DD-272B-0E2F-366E0F647126
image_variant :

Boot Details
=====
Boot mode: BIOS
Bootloader version: 1.1
```

show platform software trace filter-binary

To display the most recent trace information for a specific module, use the **show platform software trace filter-binary** command in privileged EXEC or user EXEC mode.

```
show platform software trace filter-binary modules [context mac-address]
```

| | | |
|---------------------------|-----------------------------------|--|
| Syntax Description | context <i>mac-address</i> | Represents the context used to filter. Additionally, you can filter based on module names and trace levels. The context keyword accepts either a MAC address or any other argument based on which a trace is tagged. |
|---------------------------|-----------------------------------|--|

| | |
|----------------------|--------------------------------------|
| Command Modes | User EXEC (>) Privileged EXEC (#) |
|----------------------|--------------------------------------|

| | | |
|------------------------|--------------------------------|------------------------------|
| Command History | Release | Modification |
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

| | |
|-------------------------|---|
| Usage Guidelines | This command collates and sorts all the logs present in the <code>/tmp/...</code> across all the processes relevant to the module. The trace logs of all the processes relevant to the specified module are printed to the console. This command also generates a file named <code>collated_log_{system time}</code> with the same content, in the <code>/crashinfo/tracelogs</code> directory. |
|-------------------------|---|

| | |
|-----------------|--|
| Examples | This example shows how to display the trace information for a wireless module: |
|-----------------|--|

```
Device# show platform software trace filter-binary wireless
```

show platform software trace filter-binary

To display the most recent trace information for a specific module, use the **show platform software trace filter-binary** command in privileged EXEC or user EXEC mode.

show platform software trace filter-binary *modules* [**context** *mac-address*]

| | | |
|---------------------------|-----------------------------------|--|
| Syntax Description | context <i>mac-address</i> | Represents the context used to filter. Additionally, you can filter based on module names and trace levels. The context keyword accepts either a MAC address or any other argument based on which a trace is tagged. |
|---------------------------|-----------------------------------|--|

| | |
|----------------------|--------------------------------------|
| Command Modes | User EXEC (>) Privileged EXEC (#) |
|----------------------|--------------------------------------|

| | |
|------------------------|------------------------------------|
| Command History | Release Modification |
| | This command was introduced. |

| | |
|-------------------------|--|
| Usage Guidelines | This command collates and sorts all the logs present in the <code>/tmp/.../</code> across all the processes relevant to the module. The trace logs of all the processes relevant to the specified module are printed to the console. This command also generates a file named <code>collated_log_{system time}</code> with the same content, in the <code>/crashinfo/tracelogs</code> directory. |
|-------------------------|--|

| | |
|-----------------|--|
| Examples | This example shows how to display the trace information for a wireless module: |
|-----------------|--|

```
Device# show platform software trace filter-binary wireless
```

show platform software trace level

To view the trace levels for all the modules under a specific process, use the **show platform software trace level** command in privileged EXEC or user EXEC mode.

show platform software trace level wireless [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

Syntax Description

process

Process whose tracing level is being set. Options include:

- **chassis-manager**—The Chassis Manager process.
- **cli-agent**—The CLI Agent process.
- **cmm**—The CMM process.
- **dbm**—The Database Manager process.
- **emd**—The Environmental Monitoring process.
- **fed**—The Forwarding Engine Driver process.
- **forwarding-manager**—The Forwarding Manager process.
- **geo**—The Geo Manager process.
- **host-manager**—The Host Manager process.
- **interface-manager**—The Interface Manager process.
- **iomd**—The Input/Output Module daemon (IOMd) process.
- **ios**—The IOS process.
- **license-manager**—The License Manager process.
- **logger**—The Logging Manager process.
- **platform-mgr**—The Platform Manager process.
- **pluggable-services**—The Pluggable Services process.
- **replication-mgr**—The Replication Manager process.
- **shell-manager**—The Shell Manager process.
- **sif**—The Stack Interface (SIF) Manager process.
- **smd**—The Session Manager process.
- **stack-mgr**—The Stack Manager process.
- **table-manager**—The Table Manager Server.
- **thread-test**—The Multithread Manager process.
- **virt-manager**—The Virtualization Manager process.
- **wireless**—The wireless controller module process.

| | |
|-------------|---|
| <i>slot</i> | <p>Hardware slot where the process for which the trace level is set, is running. Options include:</p> <ul style="list-style-type: none"> • <i>number</i>—Number of the SIP slot of the hardware module where the trace level is set. For instance, if you want to specify the SIP in SIP slot 2 of the switch, enter 2. • <i>SIP-slot / SPA-bay</i>—Number of the SIP switch slot and the number of the shared port adapter (SPA) bay of that SIP. For instance, if you want to specify the SPA in bay 2 of the SIP in switch slot 3, enter 3/2. • F0—The Embedded Service Processor in slot 0. • F1—The Embedded Service Processor in slot 1. • FP active—The active Embedded Service Processor. • R0—The route processor in slot 0. • RP active—The active route processor. • switch <number> —The switch, with its number specified. • switch active—The active switch. • switch standby—The standby switch. <ul style="list-style-type: none"> • <i>number</i>—Number of the SIP slot of the hardware module where the trace level is set. For instance, if you want to specify the SIP in SIP slot 2 of the switch, enter 2. • <i>SIP-slot / SPA-bay</i>—Number of the SIP switch slot and the number of the shared port adapter (SPA) bay of that SIP. For instance, if you want to specify the SPA in bay 2 of the SIP in switch slot 3, enter 3/2. • F0—The Embedded Service Processor in slot 0. • FP active—The active Embedded Service Processor. • R0—The route processor in slot 0. • RP active—The active route processor. |
|-------------|---|

Syntax Description

| | |
|-----------------------|---|
| <i>chassis-number</i> | Chassis number as either 1 or 2. |
| active R0 | Active instance of the AP filters in Route-processor slot 0. |
| standby R0 | Standby instance of the AP filters in Route-processor slot 0. |

Command Modes

User EXEC (>)
Privileged EXEC (#)

| Command History | Release | Modification |
|-----------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

Examples

This example shows how to view the trace level:

```
Device# show platform software trace level dbm switch active R0
Module Name                               Trace Level
-----
binos                                       Notice
binos/brand                               Notice
bipc                                       Notice
btrace                                     Notice
bump_ptr_alloc                             Notice
cdllib                                     Notice
chasfs                                     Notice
dbal                                       Informational
dbm                                         Debug
evlib                                       Notice
evutil                                     Notice
file_alloc                                 Notice
green-be                                   Notice
ios-avl                                    Notice
klib                                        Debug
services                                   Notice
sw_wdog                                    Notice
syshw                                       Notice
tdl_cdlcore_message                       Notice
tdl_dbal_root_message                     Notice
tdl_dbal_root_type                         Notice
```

show platform software utd chassis active F0 et-analytics global

To view the ETA global and interface details, use the **show platform software utd chassis active F0 et-analytics global** command.

show platform software utd chassis active F0 et-analytics global

| | | |
|---------------------------|--------------------------------|------------------------------|
| Syntax Description | This command has no arguments. | |
| Command Default | None | |
| Command Modes | Global configuration | |
| Command History | Release | Modification |
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the ETA global and interface details:

```
Device# show platform software utd chassis active F0 et-analytics global
ET Analytics Global Configuration
ID: 1
All Interfaces: Off
IP address and port and vrf: 192.168.5.2:2055:0
```


show platform software et-analytics global

To view the ETA global configuration, use the **show platform software et-analytics global** command.



Note The **show platform software et-analytics global** command does not display the ETA enabled wireless client interfaces.

show platform software et-analytics global

| | |
|---------------------------|--------------------------------|
| Syntax Description | This command has no arguments. |
|---------------------------|--------------------------------|

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

| | |
|----------------------|----------------------|
| Command Modes | Global configuration |
|----------------------|----------------------|

| Command History | Release | Modification |
|------------------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the ETA global and interface details:

```
Device# show platform software et-analytics global
ET-Analytics Global state
=====
All Interfaces : Off
IP Flow-record Destination: 192.168.5.2 : 2055
Inactive timer: 15
```

show platform sudi certificate

To view the checksum record for a specific SUDI, use the **show platform sudi certificate** command.

show platform sudi certificate [**sign** [**nonce** *nonce*]]

| Syntax Description | sign (Optional). Show signature. | | | | |
|-------------------------------|---|---------|--------------|-------------------------------|------------------------------|
| | nonce (Optional). Enter a nonce value. | | | | |
| Command Default | None | | | | |
| Command Modes | Privileged EXEC | | | | |
| Command History | <table border="1"> <thead> <tr> <th style="border-top: 1px solid black; border-bottom: 1px solid black;">Release</th> <th style="border-top: 1px solid black; border-bottom: 1px solid black;">Modification</th> </tr> </thead> <tbody> <tr> <td style="border-bottom: 1px solid black;">Cisco IOS XE Bengaluru 17.4.1</td> <td style="border-bottom: 1px solid black;">This command was introduced.</td> </tr> </tbody> </table> | Release | Modification | Cisco IOS XE Bengaluru 17.4.1 | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE Bengaluru 17.4.1 | This command was introduced. | | | | |

The following example shows how to view the checksum record for the specific SUDI:

```
Device# show platform sudi certificate sign nonce 123
-----BEGIN CERTIFICATE-----
MIIDQzCCAiugAwIBAgIQX/h7KCTu3I1CoxW1aMmt/zANBgkqhkiG9w0BAQUFADA1
MRYwFAYDVQQKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENB
IDIwNDgwHhcNMDQwNTE0MjAxNzEyWWhcNMjkNTE0MjAyNTQyWjA1MRYwFAYDVQQK
Ew1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwNDgwggEg
MA0GCSqGSIb3DQEBAQUAA4IBDQAwggEIAoIBAQCWmrmrp68Kd6ficba0ZmKUeIhH
xmJVhEAYv8CrLqUccda8bnuoqrpu0hWISEWdovyDOMy5jOamaHBKeN8hF570YQXJ
FcjPFto1YYmUQ6iEqDGYeJu5Tm8sUxJsZR2tKyS7McQr/4NEb7Y9JHcJ6r8qqB9q
VvYgDxFU14F1pyXOWWqCZe+36ufijXWLBvLdT6ZeYpzPEApk0E5tzivMW/VgpSdH
jWn0f84bcN5wGyDWbs2mAag8EtKpP6BrXruOIIt6ke01a06g58QBdKhTCytKmg9l
Eg6CTY5j/e/rmxxrbU6YTYK/CfdFhbBc11HP7R2RQgYCUTOG/rksc35LtLgXfAgED
o1EwTzALBgNVHQ8EBAMCAYYwDwYDVR0TAAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJ/PI
FR5umgIJFq0roIlqX9p7L6owEAYJKwYBAGCNxUBBAMCAQAwDQYJKoZIhvcNAQEF
BQADggEBAJ2dhISjQal8dwy3U8pORFbi71R803UXHOjgkxhLtv5MOhmBvRbW7hmW
Yqpao2TB9k5UM8Z3/sUcuuVdJcr18JOagxEu5sv4dEX+5wW4q+ffY0vhN4TauYuX
cB7w4ovXsNgOnbFp1iqRe6lJT37mjpxYgyc81WhJdTsd9i7rp77rMKSSh0T8lasz
Bvt9YARetIpjsJyp8qS5UwGH0GikJ3+r/+n6yUA4iGe0OcaEb1fJU9u6ju7Aq7L4
CYNu/2bPPu8Xs1gYJQk0XuPL1hS27PKSb3TkL4Eq1ZKR40CXPDJoBvYL0fdX41Id
kxpUnwVvwEpxYB5DC2Ae/qPOgRnhCzU=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEPDCCAySgAwIBAgIKYQlufQAAAAAADANBgkqhkiG9w0BAQUFADA1MRYwFAYD
VQQKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwNDgw
HhcNMTcwNjMwMjE1NjU3WWhcNMjkNTE0MjAyNTQyWjAnMQ4wDAYDVQQKEwVDaXNj
bzEVMBMGAlUEAxMMQUNUMiBTvURJiENBmIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEAM5l3THIXA9tN/hS5qR/6UZRpdd+9aE2JbFknjht6gfhKd477Aks
5XAtUs5oxDYvt/zEbs1Zq3+LR6qrqKKQV6JYvH05UYLBqCj38s76NLk53905Wzp
9pRcmRCPUx+a6tHF/qRuOiJ44mdeDYzo3qPCpxzprWJDPc1M4iYKHuMqMqmgmg+
xghHIOoWS80BOcdiynEbeP5rZ7qRuewKMpl1TiI3WdBNjZjnpfjg66F+P4SaDkGb
BXDgjl3oVeF+EyFWLrFjj97fL2+8oauV43Qrvnf3d/GfqXj7ew+z/sXLtEOjSXJ
URsyMEj53Rdd9tJwHky8neapszS+r+kdVQIDAQABo4IBWjCCAVYwCwYDVR0PBAQD
AgHGMB0GAlUdDgQWBBRI2PHxwnDVW7t8cwmTr7i4MAP4fzAfBgNVHSMEGDAWgBQn
88gVhm6aAgkWrSugiWBf2nsvqjBDBgNVHR8EPDA6MDigNqA0hjJodHRwOi8vd3d3
```

```
LmNpc2NvLmNvbS9zZWN1cm10eS9wa2kvY3JsL2NyY2EyMDQ4LmNybDBQBggrBgEF
BQCBAQREMEIwQAYIKwYBBQUHMAKGNgh0dHA6Ly93d3cuY2l2Y28uY29tL3N1Y3Vy
aXR5L3BraS9jZXJ0cy9jcmNhMjA0OC5jZXIwXAYDVR0gBFUwUzBRBgorBgEEAQkV
AQwAMEMwQQYIKwYBBQUHAgEWNWh0dHA6Ly93d3cuY2l2Y28uY29tL3N1Y3VyYXR5
L3BraS9wb2xpY2llcy9pbmRleC5odG1sMBIGA1UdEwEB/wQIMAYBAf8CAQAwdQYJ
KoZlIhvcNAQEFBQADggEBAGhlqclr9tx4hzWgDERm371yeuEmqCIfi9b9+GbMSJbi
ZHc/CcC10lJu0a9zTXA9w47H9/t61eduGxb4WeLxcwCiUgvFtCa51Ikl8nNbcKY
/4dw1ex+7amATUQO4QggIE67wVIPu6bgAE3Ja/nRS3xKYSnj8H5TehimBSv6TECi
i5jUhOWryAK4dVo8hCjkjEkzu3ufBTJapnv89g9OE+H3VKM4L+/KdkUO+52djFKn
hy147d7cZR4DY4LIuFM2P1As8YyjzoNpK/urSRI14WdIlplR1nH7KND15618yfVP
0IFJZBGrooCRBjOSwFv8cpWCbmWdPaCQT2nwIjTfY8c=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDfTCCAmWgAwIBAgIEAwQD7zANBgkqhkiG9w0BAQsFADANMQ4wDAYDVQQKEwVD
aXNjbzEVMBMGAlUEAxMMQUNUMiBTvURJIENBMB4XDTE4MDkyMzIyMzIwLjE1NDU1
MDUxNDIwMjU0MjUwVjEwMCUGA1UEBRMeUE1EOKM5NjAwLmN1bWVuc0xIFNOOKNBVDIy
MzZMMFE5MQ4wDAYDVQQKEwVDaXNjbzEYMBYGA1UECzMPQUNULTIqTG10ZSBTVURJ
MRQwEgYDVQQDEwtdOTYwMCI1TVVatMTCCASIdQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBANsh0jcvgh1pdOjP9KnffDnDc/zEHDzbCTWpJi2FzcsaSE5jvq6CUqc4
MYpNAZU2Jym7NSD8iQbMXwnCtoL64QtxQeFhRYmc4d5o933M7GwpEH0I7HUSb0/
Fxy7JBMGPPgAkY7rKsYENiNK2hiR7Q2O7X2BidOKknEuofWdJMNyMaZgLYLOhbJ
5oXaORxhUy3VRaxN16qI7kYxuugg2LcAbZ539sRXe8JtHyK811URNsgMiQ0S17pS
idGmrJJ0pEHA0EUVTzqEny3z+NW9uxLVszu6+hEJYlqfI+Yef0DbvZl1y1cy5r/jF
yNdGuGKvd5agvgCly8aYMza3P+D5S8sCAwEAaANvMG0wDgYDVR0PAQH/BAQDAgXg
MAwGA1UdEwEB/wQCMAAwTQYDVR0RBEYwRKBCBgkrBgEEAQkVAgOgNRMzQ2hpcE1E
PVUxUk5TVE13TVRjd05qSTFBQUFwZndBQUFBQUFBQUFBQUFBQUhtS1U9MAOG
CSqGSIB3DQEBcwUAA4IBAQCrpHo/CUyk5Hs/asIcYW0ep8KocSskbNh8qamyd4oWD
e/MGJW9Bs5f09IEbILWpdytCCS2lSyJbxz2HvVDzdxQdxjDwUNiWuu3dWMXN/i67
yuCGM+1A1AAG5dT6lNgWYHh+YzsZm9eoq1+4NM+JuMXWsnzAK8rSy+dSpBxqFsBq
E00lPsaK7y2h8gs+XrV9x+D48OZQkTRXpxhJfiWvs+EbdgsAM/vBxTAoTJpVmxWN
Cmcj9X52X13i4MdOUXocZLO2kh6JSgOYgkFeZifJ0iDvMfAf0cJ6+cEf6bSxAqBL
veel+8LmeiE/209h6qGHPPDacCaXA2oJCDHveAt8iPTG
-----END CERTIFICATE-----
```

Signature version: 1
Signature:

~~-----BEGIN CERTIFICATE-----~~

show platform sudi pki

To validate whether a hardware unit is programmed correctly or not, use the **show platform sudi pki** command.

show platform sudi pki

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC (#)

| Command History | Release | Modification |
|-----------------|-------------------------------|------------------------------|
| | Cisco IOS XE Cupertino 17.7.1 | This command was introduced. |

Examples

The following example shows how to check whether a hardware unit is programmed correctly or not:

```
Device# show platform sudi pki
```

```
CMCA3 cert status : Enabled / Disabled
```

```

SUDI Issuer                               Validity status
-----
Cisco Manufacturing CA III                 Valid / Not-valid
Cisco Manufacturing CA SHA2               Valid / Not-valid
Cisco Manufacturing CA                     Valid / Not-valid

```

show parameter-map type umbrella global

To view the Umbrella global parameter map details, use the **show parameter-map type umbrella global** command.

```
show parameter-map type umbrella global
```

| Syntax Description | This command has no arguments. | | | | |
|--------------------------------|--|---------|--------------|--------------------------------|------------------------------|
| Command Default | None | | | | |
| Command Modes | Global configuration | | | | |
| Command History | <table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>Cisco IOS XE Gibraltar 16.10.1</td><td>This command was introduced.</td></tr></tbody></table> | Release | Modification | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. | | | | |

This example shows how to view the Umbrella global parameter map details:

```
Device# show parameter-map type umbrella global
parameter-map type umbrella global
  token 57CC80106C087FB1B2A7BAB4F2F4373C00247166
  local-domain dns_wl
  dnscrypt
  udp-timeout 2
  resolver ipv4 208.67.220.220
  resolver ipv4 208.67.222.222
  resolver ipv6 2620:119:53::53
  resolver ipv6 2620:119:35::35
```

show policy-map

To display quality of service (QoS) policy maps, which define classification criteria for incoming traffic, use the **show policy-map** command in EXEC mode.

```
show policy-map [{policy-map-name | interface interface-id}]
```

```
show policy-map interface {Auto-template | Capwap | GigabitEthernet | GroupVI |
InternalInterface | Loopback | Lspvif | Null | Port-channel | TenGigabitEthernet | Tunnel
| Vlan | brief | class | input | output
```

```
show policy-map interface {ap name ap_name | client mac mac_address | radio type {24ghz |
5ghz} ap name ap_name | ssid name ssid_name {ap name ap_name | radio type {24ghz | 5ghz}
ap name ap_name } }
```

Syntax Description

| | |
|--|--|
| <i>policy-map-name</i> | (Optional) Name of the policy-map. |
| interface <i>interface-id</i> | (Optional) Displays the statistics and the configurations of the input and output policies that are attached to the interface. |
| ap name <i>ap_name</i> | Displays SSID policy configuration of an access point. |
| client mac <i>mac_address</i> | Displays information about the policies for all the client targets. |
| radio type { 24ghz 5ghz } | Displays policy configuration of the access point in the specified radio type. |
| ssid name <i>ssid_name</i> | Displays policy configuration of an SSID. |

Command Modes

User EXEC
Privileged EXEC

Command History

| Release | Modification |
|--------------------------------|----------------|
| Cisco IOS XE Gibraltar 16.10.1 | This command w |

Usage Guidelines

Policy maps can include policers that specify the bandwidth limitations and the action to take if the limits are exceeded.



Note Though visible in the command-line help string, the **control-plane**, **session**, and **type** keywords are not supported, and the statistics shown in the display should be ignored.

To display classification counters for ternary content addressable memory (TCAM) (marking or policing) based policies, enter the interface ID. Classification counters have the following restrictions:

- Classification counters are supported only on wired ports (in the ingress and egress directions).
- Classification counters count packets instead of bytes.
- Only QoS configurations with marking or policing trigger the classification counter.
- As long as there is policing or marking action in the policy, the class-default will have classification counters.
- Classification counters are not port based. The counters are shared across targets sharing the same policy map. This means that the classification counter aggregates all packets belonging to the same class of the same policy which attach to different interfaces.

This is an example of output from the **show policy-map interface** command, where classification counters are displayed:

```
Device# show policy-map interface gigabitethernet1/0/1

GigabitEthernet1/0/1

Service-policy input: AutoQos-4.0-CiscoPhone-Input-Policy

Class-map: AutoQos-4.0-Voip-Data-CiscoPhone-Class (match-any)
  0 packets
  Match: cos 5
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp ef
  police:
    cir 128000 bps, bc 8000 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      set-dscp-transmit dscp table policed-dscp
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Voip-Signal-CiscoPhone-Class (match-any)
  0 packets
  Match: cos 3
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp cs3
  police:
    cir 32000 bps, bc 8000 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      set-dscp-transmit dscp table policed-dscp
    conformed 0000 bps, exceed 0000 bps
```

```

Class-map: AutoQos-4.0-Default-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-Default
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp default

Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets, 0 bytes
    5 minute rate 0 bps

Service-policy output: AutoQos-4.0-Output-Policy

queue stats for all priority classes:
  Queueing
  priority level 1

  (total drops) 0
  (bytes output) 0

Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
  0 packets
  Match: dscp cs4 (32) cs5 (40) ef (46)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 5
    0 packets, 0 bytes
    5 minute rate 0 bps
  Priority: 30% (300000 kbps), burst bytes 7500000,

  Priority Level: 1

Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
  0 packets
  Match: dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 3
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing
  queue-limit dscp 16 percent 80
  queue-limit dscp 24 percent 90
  queue-limit dscp 48 percent 100
  queue-limit dscp 56 percent 100

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%

  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
  0 packets
  Match: dscp af41 (34) af42 (36) af43 (38)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 4
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

```



```
(total drops) 0
(bytes output) 0
bandwidth remaining 10%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
 0 packets
Match: dscp af21 (18) af22 (20) af23 (22)
 0 packets, 0 bytes
 5 minute rate 0 bps
Match: cos 2
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 10%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
 0 packets
Match: dscp af11 (10) af12 (12) af13 (14)
 0 packets, 0 bytes
 5 minute rate 0 bps
Match: cos 1
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 4%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
 0 packets
Match: dscp cs1 (8)
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 1%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
 0 packets
Match: dscp af31 (26) af32 (28) af33 (30)
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 10%
queue-buffers ratio 10

Class-map: class-default (match-any)
 0 packets
Match: any
 0 packets, 0 bytes
```

```
5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 25%
queue-buffers ratio 25
```

show processes cpu

To display detailed CPU utilization statistics of IOS tasks, use the **show processes cpu** command.

show processes cpu [**autoprofile** | **extended** | **history** [**table**] | **sorted** [**1min** | **5min** | **5sec**]]

Syntax Description

| | |
|--------------------|--|
| autoprofile | (Optional) Displays IOS(d) 'automatic CPUHOG profiling' information. |
| extended | (Optional) Displays extended CPU usage report of last 5 seconds for IOS(d) process. |
| history | (Optional) Displays CPU history in a graph format. |
| table | (Optional) Displays CPU history in a table format. |
| sorted | (Optional) For Cisco IOS images only. Displays CPU utilization sorted by percentage. |
| history | (Optional) Sorts CPU utilization history. See Usage Guidelines for details. |
| 1min | (Optional) Sorts CPU utilization based on 1-minute utilization. |
| 5min | (Optional) Sorts CPU utilization based on 5-minute utilization. |
| 5sec | (Optional) Sorts CPU utilization based on 5-second utilization. |

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

| Release | Modification |
|-------------------------------|---|
| Cisco IOS XE Amsterdam 17.3.1 | This command was integrated into Cisco IOS XE Amsterdam 17.3.1. |

Usage Guidelines

If you use the **history** keyword, three graphs are displayed for Cisco IOS images:

- CPU utilization for the last 60 seconds
- CPU utilization for the last 60 minutes
- CPU utilization for the last 72 hours

Maximum usage is measured and recorded every second. The average usage is calculated on periods of more than one second. Consistently high CPU utilization over an extended period indicates a problem.

To enable standby console, ensure that the following configuration is in place:

```
redundancy
main-cpu
secondary console enable
```

Example

The following is a sample output from the **show processes cpu** command without keywords:

show processes cpu

```
Device# show processes cpu
```

```
CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
PID Runtime(ms)   Invoked    uSecs   5Sec   1Min   5Min  TTY Process
  10   1576556       281188    5606   0.15%  0.05%  0.05%  0 Check heaps
 232   845057       54261160   15    0.07%  0.05%  0.06%  0 IPAM Manager
 595    177         300       590   0.07%  0.02%  0.01%  2 Virtual Exec
 138  1685973     108085955   15    0.07%  0.08%  0.08%  0 L2 LISP Punt Pro
 193   19644       348767     56    0.07%  0.00%  0.00%  0 DTP Protocol
   5     0           1         0    0.00%  0.00%  0.00%  0 CTS SGACL db cor
   4    24          15       1600  0.00%  0.00%  0.00%  0 RF Slave Main Th
   6     0           1         0    0.00%  0.00%  0.00%  0 Retransmission o
   7     0           1         0    0.00%  0.00%  0.00%  0 IPC ISSU Dispatc
   2   117631     348801    337   0.00%  0.00%  0.00%  0 Load Meter
   8     0           1         0    0.00%  0.00%  0.00%  0 EDDRI_MAIN
.
.
.
```

show rate-limit client

To configure the rate-limit for a client on the AP, use the **show rate-limit client** command.

show rate-limit client

| | | |
|---------------------------|--------------------------------|------------------------------|
| Syntax Description | This command has no arguments. | |
| Command Modes | Privileged EXEC (#) | |
| Command History | Release | Modification |
| | Cisco IOS XE Gibraltar 16.12.1 | This command was introduced. |

The following example shows how to configure the rate-limit for a client on the AP:

```
Device# show rate-limit client
Config:
mac vap rt_rate_out rt_rate_in rt_burst_out rt_burst_in nrt_rate_out nrt_rate_in nrt_burst_out
  nrt_burst_in
00:1C:F1:09:85:E7 0 8001 8002 8003 8004 8005 8006 8007 8008
Statistics:
name up down
Unshaped 0 0
Client RT pass 0 0
Client NRT pass 0 0
Client RT drops 0 0
Client NRT drops 0 0
Per client rate limit:
mac vap rate_out rate_in policy
```

show remote-lan all

To view the detailed output of all RLANs, use the **show remote-lan all** command.

show remote-lan all

| Command Default | None | | | | |
|--------------------------------|--|---------|--------------|--------------------------------|------------------------------|
| Command Modes | Global configuration | | | | |
| Command History | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.10.1</td> <td>This command was introduced.</td> </tr> </tbody> </table> | Release | Modification | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. | | | | |

This example shows how to view the detailed output of all RLANs:

```
Device# show remote-lan all
Remote-LAN Profile Name      : rlan_test_1
=====
Identifier                   : 1
Status                       : Enabled
Mac-filtering                : Not Configured
Number of Active Clients     : 1
Security_8021X               : Disabled
8021.x Authentication list name : Not Configured
Local Auth eap Profile Name  : Not Configured
Web Auth Security            : Disabled
Webauth Authentication list name : Not Configured
Web Auth Parameter Map      : Not Configured
Client association limit     : 0
Ipv4 Web Pre Auth Acl       : Not Configured
Ipv6 Web Pre Auth Acl       : Not Configured

Remote-LAN Profile Name      : rlan_test_2
=====
Identifier                   : 2
Status                       : Enabled
Mac-filtering                : Not Configured
Number of Active Clients     : 1
Security_8021X               : Disabled
8021.x Authentication list name : Not Configured
Local Auth eap Profile Name  : Not Configured
Web Auth Security            : Disabled
Webauth Authentication list name : Not Configured
Web Auth Parameter Map      : Not Configured
Client association limit     : 0
Ipv4 Web Pre Auth Acl       : Not Configured
Ipv6 Web Pre Auth Acl       : Not Configured
```

show remote-lan id

To view the RLAN configuration by ID, use the **show remote-lan id** command.

```
show remote-lan id id
```

Command Default

None

Command Modes

Global configuration

Command History

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

This example shows how to view the RLAN configuration by ID:

```
Device# show remote-lan id <id>
Remote-LAN Profile Name      : rlan_test_1
=====
Identifier                    : 1
Status                        : Enabled
Mac-filtering                 : Not Configured
Number of Active Clients      : 1
Security_8021X                : Disabled
8021.x Authentication list name : Not Configured
Local Auth eap Profile Name   : Not Configured
Web Auth Security             : Disabled
Webauth Authentication list name : Not Configured
Web Auth Parameter Map        : Not Configured
Client association limit      : 0
Ipv4 Web Pre Auth Acl         : Not Configured
Ipv6 Web Pre Auth Acl         : Not Configured
```

show remote-lan name

To view the RLAN configuration by profile name, use the **show remote-lan name** command.

show remote-lan name *profile-name*

| Command Default | None | | | | |
|--------------------------------|--|---------|--------------|--------------------------------|------------------------------|
| Command Modes | Global configuration | | | | |
| Command History | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.10.1</td> <td>This command was introduced.</td> </tr> </tbody> </table> | Release | Modification | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. | | | | |

This example shows how to view the RLAN configuration by profile name:

```
Device# show remote-lan name <profile-name>
Remote-LAN Profile Name      : rlan_test_1
=====
Identifier                    : 1
Status                        : Enabled
Mac-filtering                 : Not Configured
Number of Active Clients      : 1
Security_8021X                : Disabled
8021.x Authentication list name : Not Configured
Local Auth eap Profile Name   : Not Configured
Web Auth Security             : Disabled
Webauth Authentication list name : Not Configured
Web Auth Parameter Map        : Not Configured
Client association limit      : 0
Ipv4 Web Pre Auth Acl         : Not Configured
Ipv6 Web Pre Auth Acl         : Not Configured
```


show remote-lan policy detail

To view the RLAN policy profile details by profile name, use the **show remote-lan policy detail** command.

```
show remote-lan policy detail rlan_profile_name
```

Command Default None

Command Modes Global configuration

| Command History | Release | Modification |
|-----------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the RLAN policy profile details by profile name:

```
Device# show remote-lan policy detail <rlan_profile_name>
Profile Name           : rlan_named_ppl
Status                 : Enabled
Description            :
REMOTE-LAN ACL
  IPv4 ACL name        : Not Configured
  IPv6 ACL name        : Not Configured
AAA Policy Params
  AAA Override         : Disabled
  AAA Policy name      : default-aaa-policy
RLAN Switching policy
  Central Switching    : Enabled
  Central Dhcp         : Enabled
VLAN                   : 20
Pre Authentication     : Disabled
Session Time out      : 1800
Violation Mode         : REPLACE
Host Mode              : SINGLE_HOST_MODE
Host mode VLANs
  Voice Vlan Id        : Not Configured
  Data Vlan Id         : Not Configured
Exclusionlist Params
  Exclusionlist         : Enabled
  Exclusion Timeout     : 60
Flow Monitor IPv4
  Flow Monitor Ingress Name : Not Configured
  Flow Monitor Egress Name  : Not Configured
  Flow Monitor Ingress status : Disabled
  Flow Monitor egress status : Disabled
Flow Monitor IPv6
  Flow Monitor Ingress Name : Not Configured
  Flow Monitor Egress Name  : Not Configured
  Flow Monitor Ingress status : Disabled
  Flow Monitor egress status : Disabled
Split Tunnel Parameters
  Status               : Disabled
  ACL name             : Not Configured
  Override Status      : Disabled
  Gateway Address      : Not Configured
  Netmask Address      : Not Configured
DHCP
```

show remote-lan policy detail

```
DHCP Required           : Disabled
DHCP Server             : Not Configured
Accounting List         : Not Configured
```

show remote-lan policy summary

To view the summary of policy profile for all RLANs, use the **show remote-lan policy summary** command.

```
show remote-lan policy summary
```

Command Default None

Command Modes Global configuration

Command History

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

This example shows how to view the summary of policy profile for all RLANs:

```
Device# show remote-lan policy summary
Number of Policy Profiles: 1
```

| Profile Name | Description | Status |
|----------------|-----------------------------|---------|
| rlan_named_pp1 | Testing RLAN policy profile | Enabled |

show remote-lan summary

To view the summary of all RLANs, use the **show remote-lan summary** command.

show remote-lan summary

Syntax Description This command has no arguments.

Command Default None

Command Modes Global configuration

| Command History | Release | Modification |
|-----------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the summary of all RLANs:

```
Device# show remote-lan summary
Number of RLANs: 1
```

| RLAN | Profile Name | Status |
|------|--------------|---------|
| 1 | rlan_test_1 | Enabled |

show sdavc ap download status

To view the per access point (per-AP) download status for Software-Defined Application Visibility and Control (SD-AVC), use the **show sdavc ap download status** command.

show sdavc ap download status

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC (#)

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

Examples

The following example shows how to view the per-AP download status for SD-AVC:

```
Device# show sdavc ap download status
```

```
AP  MAC           Latest filename  Status
-----
00d7.8f58.2f80    xyz              SUCCESS
00d7.8f58.2d82    abc              FAILED
```

show sdavc status ap

To view the Software-Defined Application Visibility and Control (SD-AVC) status for an access point (AP), use the **show sdavc status ap** command.

show sdavc status ap *ap-name*

| | |
|---------------------------|--|
| Syntax Description | <i>ap-name</i> AP name or MAC address. |
|---------------------------|--|

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

| | |
|----------------------|---------------------|
| Command Modes | Privileged EXEC (#) |
|----------------------|---------------------|

| Command History | Release | Modification |
|------------------------|-------------------------------|------------------------------|
| | Cisco IOS XE Cupertino 17.7.1 | This command was introduced. |

Examples

The following example shows how to view the SD-AVC status for an AP:

```
Device# show sdavc status ap 00d7.8f58.2f80

AP MAC                               Status
-----
00d7.8f58.2f80                       ENABLED
```

show ssh

To see the SSH connection status, use the **show ssh** command.

```
show ssh {connection-number | {vtty connection-number } }
```

Syntax Description

connection-number SSH connection number. Valid range is 0 to 530.

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Examples

The following example shows how to see the SSH connection status:

```
Device# show ssh connection-number
```

show split-tunnel client access-list

To verify split tunneling Domain Name System (DNS) Access Control Lists (ACLs) per wireless client, use the **show split-tunnel client access-list** command.

show split-tunnel client *mac-address* **access-list**

| Syntax Description | |
|--------------------|---|
| | <i>mac-address</i> Wireless client MAC address. |

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

| Command Modes | |
|---------------|---------------------|
| | Privileged EXEC (#) |

| Command History | Release | Modification |
|-----------------|-------------------------------|------------------------------|
| | Cisco IOS XE Cupertino 17.1.1 | This command was introduced. |

Examples

The following example shows how to verify the split tunneling DNS ACLs for a wireless client:

```
Device# show split-tunnel client 00:11:22:33:44:55 access-list

Split tunnel ACLs for Client: 00:11:22:33:44:55

IP ACL: SplitTunnelACL

Tunnel packets Tunnel bytes NAT packets NAT bytes
           1           242           3           768

URL ACL: SplitTunnelACL

Tunnel packets Tunnel bytes NAT packets NAT bytes
           3           778           0           0

Resolved IPs for Client: 00:11:22:33:44:55 for Split tunnel

HIT-COUNT      URL                ACTION  IP-LIST
-----
1              base1.com          deny.   209.165.200.224
              base1.com          deny.   209.165.200.225
2              base2.com          deny.   209.165.200.226
3              base3.com          deny.   209.165.200.227
```


show tech-support wireless

To display Cisco wireless LAN controller variables frequently requested by Cisco Technical Assistance Center (TAC), use the **show tech-support wireless** command in privileged EXEC mode.

show tech-support wireless

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

The following is sample output from the **show tech-support wireless** command:

```
Device# show tech-support wireless
*** show ap capwap timers ***

Cisco AP CAPWAP timers

AP Discovery timer           : 10
AP Heart Beat timeout       : 30
Primary Discovery timer     : 120
Primed Join timeout         : 0
Fast Heartbeat              : Disabled
Fast Heartbeat timeout     : 1
*** show ap capwap retransmit ***
Global control packet retransmit interval : 3
Global control packet retransmit count : 5

AP Name                      Retransmit Interval      Retransmit Count
-----
TSIM_AP-2                    3                          5
TSIM_AP-3                    3                          5
*** show ap dot11 24ghz cleanair air-quality summary ***

AQ = Air Quality
DFS = Dynamic Frequency Selection

*** show ap dot11 24ghz cleanair air-quality worst ***

AQ = Air Quality
DFS = Dynamic Frequency Selection
AP Name      Channel  Avg AQ  Min AQ  Interferers  DFS
-----
              0         0       0       0             0       No
*** show ap dot11 24ghz cleanair config ***

Clean Air Solution..... : Disabled
Air Quality Settings:
  Air Quality Reporting..... : Disabled
  Air Quality Reporting Period (min)..... : 15
```

```

Air Quality Alarms..... : Enabled
Air Quality Alarm Threshold..... : 10
Interference Device Settings:
  Interference Device Reporting..... : Enabled
    Bluetooth Link..... : Enabled
    Microwave Oven..... : Enabled
    802.11 FH..... : Enabled
    Bluetooth Discovery..... : Enabled
    TDD Transmitter..... : Enabled
    Jammer..... : Enabled
    Continuous Transmitter..... : Enabled
    DECT-like Phone..... : Enabled
    Video Camera..... : Enabled
    802.15.4..... : Enabled
    WiFi Inverted..... : Enabled
    WiFi Invalid Channel..... : Enabled
    SuperAG..... : Enabled
    Canopy..... : Enabled
    Microsoft Device..... : Enabled
    WiMax Mobile..... : Enabled
    WiMax Fixed..... : Enabled
  Interference Device Types Triggering Alarms:
    Bluetooth Link..... : Disabled
    Microwave Oven..... : Disabled
    802.11 FH..... : Disabled
    Bluetooth Discovery..... : Disabled
    TDD Transmitter..... : Disabled
    Jammer..... : Disabled
    Continuous Transmitter..... : Disabled
    DECT-like Phone..... : Disabled
    Video Camera..... : Disabled
    802.15.4..... : Disabled
    WiFi Inverted..... : Enabled
    WiFi Invalid Channel..... : Enabled
    SuperAG..... : Disabled
    Canopy..... : Disabled
    Microsoft Device..... : Disabled
    WiMax Mobile..... : Disabled
    WiMax Fixed..... : Disabled
  Interference Device Alarms..... : Enabled
Additional Clean Air Settings:
  CleanAir Event-driven RRM State..... : Disabled
  CleanAir Driven RRM Sensitivity..... : LOW
  CleanAir Persistent Devices state..... : Disabled

```

show tech-support wireless ap

To display specific information about the Cisco APs variables frequently requested by Cisco Technical Assistance Center (TAC), use the **show tech-support wireless ap** command in privileged EXEC mode.

show tech-support wireless ap

| | | |
|---------------------------|--|------------------------------|
| Syntax Description | This command has no arguments or keywords. | |
| Command Default | None | |
| Command Modes | Privileged EXEC (#) | |
| Command History | Release | Modification |
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

Usage Guidelines The output of the following commands are displayed as part of **show tech-support wireless ap** command:

- show ap session termination statistics
- show ap status
- show ap tag summary
- show platform software bssid chassis active F0 statistics
- show platform software bssid chassis active R0 statistics
- show platform software capwap chassis active F0 statistics
- show platform software capwap chassis active R0 statistics
- show platform software dtls chassis active F0 statistics
- show platform software dtls chassis active R0 statistics
- show platform software radio chassis active F0 statistics
- show platform software radio chassis active R0 statistics

Example

The following is sample output from the **show tech-support wireless ap** command

```
Device# show tech-support wireless ap
----- show platform software dtls chassis active R0 statistics -----
DTLS Counters      (Success/Failure)
-----
Create              0/0
```

```
Delete                0/0
```

```
Switch 1:
OM Create              0/0
OM Delete              0/0
Ack Nack Notify       0/0
```

```
----- show platform software radio chassis active R0 statistics
-----
```

```
Switch 1:
NACK Notify           0/0
  Create Failure      0
  Delete Failure      0
```

```
----- show platform software bssid chassis active R0 statistics
-----
```

```
Switch 1:
NACK Notify           0/0
  Create Failure      0
  Delete Failure      0
```

```
----- show platform software capwap chassis active R0 statistics
-----
```

```
Capwap Counters      (Success/Failure)
-----
```

```
Create                0/0
Delete                0/0
Modify                0/0
```

```
Switch 1:
OM Create              0/0
OM Delete              0/0
ACK-NACK Notify       0/0
  Tunnel State        0/0
  Tunnel Create       0/0
  Tunnel Modify       0/0
  Tunnel Delete       0/0
```

```
----- show platform software dtls chassis active F0 statistics -----
```

```
DTLS Counters        (Success/Failure)
-----
```

```
Create                0/0
Delete                0/0
HW Create              0/0
HW Modify              0/0
HW Delete              0/0
Create Ack             0/0
Modify Ack             0/0
Delete Ack             0/0
Ack Ack Notify        0/0
```

```

Ack Nack Notify      0/0
Nack Notify          0/0
HA Seq GET           665/0
HA Seq SET           0/0
HA Seq Crypto GET    0/0
HA Seq Crypto SET    0/0
HA Seq Crypto Callback 0/0

```

```

HA Seq last Responded 0
HA Seq Pending         0
HA Seq Outstanding cb 0

```

```

----- show platform software radio chassis active F0 statistics
-----

```

```

Radio Counters      (Success/Failure)
-----

```

```

Create              0/0
Delete              0/0
HW Create           0/0
HW Modify           0/0
HW Delete           0/0
Create Ack          0/0
Modify Ack          0/0
Delete Ack          0/0
Nack Notify         0/0

```

```

----- show platform software bssid chassis active F0 statistics
-----

```

```

Bssid Counters      (Success/Failure)
-----

```

```

Create              0/0
Delete              0/0
HW Create           0/0
HW Modify           0/0
HW Delete           0/0
Create Ack          0/0
Modify Ack          0/0
Delete Ack          0/0
Nack Notify         0/0

```

```

----- show platform software capwap chassis active F0 statistics
-----

```

```

Capwap Counters     (Success/Failure)
-----

```

```

Create              0/0
Delete              0/0
HW Create           0/0
HW Modify           0/0
HW Delete           0/0
Create Ack          0/0
Modify Ack          0/0
Delete Ack          0/0
Ack Ack Notify     0/0
Ack Nack Notify    0/0
Nack Notify         0/0

```

```
----- show ap auto-rf dot11 24ghz -----
```

```
----- show ap auto-rf dot11 5ghz -----
```

```
----- show ap capwap retransmit -----
```

```
----- show ap config dot11 dual-band summary -----
```

```
----- show ap config general -----
```

```
----- show ap dot11 24ghz channel -----
```

Leader Automatic Channel Assignment

```
Channel Assignment Mode           : AUTO
Channel Update Interval          : 600 seconds
Anchor time (Hour of the day)    : 0
Channel Update Contribution
  Noise                           : Enable
  Interference                     : Enable
  Load                            : Disable
  Device Aware                     : Disable
CleanAir Event-driven RRM option : Disabled
Channel Assignment Leader        : ewlc-doc (9.12.32.10)
Last Run                          : 25 seconds ago
```

```
DCA Sensitivity Level             : MEDIUM : 10 dB
DCA Minimum Energy Limit         : -95 dBm
Channel Energy Levels
  Minimum                         : unknown
  Average                         : unknown
  Maximum                         : -128 dBm
Channel Dwell Times
  Minimum                         : unknown
  Average                         : unknown
```

```
----- show ap dot11 24ghz group -----
```

Radio RF Grouping

```
802.11b Group Mode               : AUTO
802.11b Group Update Interval    : 600 seconds
802.11b Group Leader             : ewlc-doc (9.12.32.10)
802.11b Last Run                 : 26 seconds ago
```

RF Group Members

```
Controller name                   Controller IP
```

```

-----
ewlc-doc                               9.12.32.10

----- show ap dot11 24ghz load-info -----

----- show ap dot11 24ghz monitor -----

Default 802.11b AP monitoring
 802.11b Monitor Mode                : Enabled
 802.11b Monitor Channels             : Country channels
 802.11b RRM Neighbor Discover Type   : Transparent
 802.11b AP Coverage Interval        : 180 seconds
 802.11b AP Load Interval            : 60 seconds
 802.11b AP Noise Interval           : 180 seconds
 802.11b AP Signal Strength Interval : 60 seconds
 802.11b NDP RSSI Normalization      : Enabled

----- show ap dot11 24ghz network -----

802.11b Network                      : Enabled
11gSupport                           : Enabled
11nSupport                           : Enabled
802.11b/g Operational Rates
 802.11b 1M                          : Mandatory
 802.11b 2M                          : Mandatory
 802.11b 5.5M                        : Mandatory
 802.11b 11M                         : Mandatory
 802.11g 6M                          : Supported
 802.11g 9M                          : Supported
 802.11g 12M                         : Supported
 802.11g 18M                         : Supported
 802.11g 24M                         : Supported
 802.11g 36M                         : Supported
 802.11g 48M                         : Supported
 802.11g 54M                         : Supported
802.11n MCS Settings:
MCS 0 : Supported
MCS 1 : Supported
MCS 2 : Supported
MCS 3 : Supported

----- show ap dot11 24ghz profile -----

Default 802.11b AP performance profiles
 802.11b Global Interference threshold : 10 %
 802.11b Global noise threshold       : -70 dBm
 802.11b Global RF utilization threshold : 80 %
 802.11b Global throughput threshold  : 1000000 bps
 802.11b Global clients threshold     : 12 clients

----- show ap dot11 24ghz summary -----

```

```
----- show ap dot11 24ghz txpower -----
```

Automatic Transmit Power Assignment

```

Transmit Power Assignment Mode      : AUTO
Transmit Power Update Interval      : 600 seconds
Transmit Power Threshold             : -70 dBm
Transmit Power Neighbor Count        : 3 APs
Min Transmit Power                   : -10 dBm
Max Transmit Power                   : 30 dBm
Update Contribution
  Noise                               : Enable
  Interference                         : Enable
  Load                                : Disable
  Device Aware                         : Disable
Transmit Power Assignment Leader     : ewlc-doc (9.12.32.10)
Last Run                              : 27 seconds ago

```

```
----- show ap dot11 5ghz channel -----
```

Leader Automatic Channel Assignment

```

Channel Assignment Mode              : AUTO
Channel Update Interval              : 600 seconds
Anchor time (Hour of the day)        : 0
Channel Update Contribution
  Noise                               : Enable
  Interference                         : Enable
  Load                                : Disable
  Device Aware                         : Disable
CleanAir Event-driven RRM option     : Disabled
Channel Assignment Leader             : ewlc-doc (9.12.32.10)
Last Run                              : 27 seconds ago

DCA Sensitivity Level                 : MEDIUM : 15 dB
DCA 802.11n/ac Channel Width         : 20 MHz
DCA Minimum Energy Limit              : -95 dBm
Channel Energy Levels
  Minimum                             : unknown
  Average                             : unknown
  Maximum                             : -128 dBm
Channel Dwell Times
  Minimum                             : unknown

```

```
----- show ap dot11 5ghz group -----
```

Radio RF Grouping

```

802.11a Group Mode                   : AUTO
802.11a Group Update Interval        : 600 seconds
802.11a Group Leader                 : ewlc-doc (9.12.32.10)
802.11a Last Run                     : 28 seconds ago

```

RF Group Members

```

Controller name                      Controller IP

```



```

-----
ewlc-doc                               9.12.32.10

----- show ap dot11 5ghz load-info -----

----- show ap dot11 5ghz monitor -----

Default 802.11a AP monitoring
 802.11a Monitor Mode                   : Enabled
 802.11a Monitor Channels                : Country channels
 802.11a RRM Neighbor Discover Type      : Transparent
 802.11a AP Coverage Interval           : 180 seconds
 802.11a AP Load Interval                : 60 seconds
 802.11a AP Noise Interval               : 180 seconds
 802.11a AP Signal Strength Interval     : 60 seconds
 802.11a NDP RSSI Normalization          : Enabled

----- show ap dot11 5ghz network -----

802.11a Network                         : Enabled
11nSupport                               : Enabled
 802.11a Low Band                       : Enabled
 802.11a Mid Band                        : Enabled
 802.11a High Band                      : Enabled
802.11a Operational Rates
 802.11a 6M                             : Mandatory
 802.11a 9M                             : Supported
 802.11a 12M                            : Mandatory
 802.11a 18M                            : Supported
 802.11a 24M                            : Mandatory
 802.11a 36M                            : Supported
 802.11a 48M                            : Supported
 802.11a 54M                            : Supported
802.11n MCS Settings:
MCS 0 : Supported
MCS 1 : Supported
MCS 2 : Supported
MCS 3 : Supported
MCS 4 : Supported
MCS 5 : Supported

----- show ap dot11 5ghz profile -----

Default 802.11a AP performance profiles

 802.11a Global Interference threshold   : 10 %
 802.11a Global noise threshold          : -70 dBm
 802.11a Global RF utilization threshold  : 80 %
 802.11a Global throughput threshold     : 1000000 bps
 802.11a Global clients threshold        : 12 clients

----- show ap dot11 5ghz summary -----

```

```
----- show ap dot11 5ghz txpower -----
```

```
Automatic Transmit Power Assignment
```

```
Transmit Power Assignment Mode      : AUTO
Transmit Power Update Interval      : 600 seconds
Transmit Power Threshold             : -70 dBm
Transmit Power Neighbor Count       : 3 APs
Min Transmit Power                  : -10 dBm
Max Transmit Power                  : 30 dBm
Update Contribution
  Noise                             : Enable
  Interference                       : Enable
  Load                               : Disable
  Device Aware                       : Disable
Transmit Power Assignment Leader     : ewlc-doc (9.12.32.10)
Last Run                             : 28 seconds ago
```

```
----- show ap image -----
```

```
----- show wireless stats ap join summary -----
```

```
Number of APs: 0
```

| Base MAC | Ethernet MAC | AP Name | IP Address | Status |
|-------------------|------------------------|---------|------------|--------|
| Last Failure Type | Last Disconnect Reason | | | |

```
----- show ap rf-profile summary -----
```

```
Number of RF-profiles: 6
```

| RF Profile Name | Band | Description | State |
|--------------------------------|---------|--------------------------------------|-------|
| Low_Client_Density_rf_5gh | 5 GHz | pre configured Low Client Density rf | Up |
| High_Client_Density_rf_5gh | 5 GHz | pre configured High Client Density r | Up |
| Low_Client_Density_rf_24gh | 2.4 GHz | pre configured Low Client Density rf | Up |
| High_Client_Density_rf_24gh | 2.4 GHz | pre configured High Client Density r | Up |
| Typical_Client_Density_rf_5gh | 5 GHz | pre configured Typical Density rfpro | Up |
| Typical_Client_Density_rf_24gh | 2.4 GHz | pre configured Typical Client Densit | Up |

```
----- show ap slots -----
```

```
----- show ap summary -----
```

```
Number of APs: 0
```

----- show ap uptime -----

Number of APs: 0

----- show ap tag summary -----

Number of APs: 0

----- show ap status -----

----- show ap cdp neighbors -----

Number of neighbors: 0

----- show ap ap-join-profile summary -----

Number of AP Profiles: 1

| AP Profile Name | Description |
|--------------------|--------------------|
| default-ap-profile | default ap profile |

----- show ap link-encryption -----

----- show wireless stats ap session termination -----

----- show wireless loadbalance ap affinity wncd 0 -----

----- show wireless loadbalance ap affinity wncd 1 -----

----- show wireless loadbalance ap affinity wncd 2 -----

----- show wireless loadbalance ap affinity wncd 3 -----

----- show wireless loadbalance ap affinity wncd 4 -----

----- show wireless loadbalance ap affinity wncd 5 -----

```
----- show wireless loadbalance ap affinity wncd 6 -----
```

```
----- show wireless loadbalance ap affinity wncd 7 -----
```

show tech-support wireless client

To print the data related to all clients or a particular client, use the **show tech-support wireless client** command in privileged EXEC mode.

show tech-support wireless client

| Syntax Description | mac-address Client MAC address. | | | | |
|--------------------------------|--|---------|--------------|--------------------------------|------------------------------|
| Command Default | None | | | | |
| Command Modes | Privileged EXEC (#) | | | | |
| Command History | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.10.1</td> <td>This command was introduced.</td> </tr> </tbody> </table> | Release | Modification | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. | | | | |

Usage Guidelines The output of the following commands are displayed as part of **show tech-support wireless client** command:

- show platform software wireless-client chassis active F0 statistics
- show platform software wireless-client chassis active R0 statistics
- show wireless client calls active
- show wireless client calls rejected
- show wireless client client-statistics summary
- show wireless client device summary
- show wireless client mac <mac-addr> details
- show wireless client probing
- show wireless client sleeping-client
- show wireless client statistic
- show wireless client steering
- show wireless client summary
- show wireless exclusionlist
- show wireless pmk-cache



Note The **show tech-support wireless client** command does not display the output of **show wireless client summary detail** command.

Example

The following is sample output from the **show tech-support wireless client** command

```

Device# show tech-support wireless client

----- show wireless stats client summary -----

Number of Local Clients : 0

MAC Address      AP Name          WLAN UpTime(secs) Rx Pkts Tx Pkts RSSI SNR
Data Retries
-----

----- show wireless client summary -----

Number of Local Clients: 0

Number of Excluded Clients: 0

----- show wireless client device summary -----

----- show wireless client steering -----

Client Steering Configuration Information
Macro to micro transition threshold      : -55 dBm
Micro to Macro transition threshold     : -65 dBm
Micro-Macro transition minimum client count : 3
Micro-Macro transition client balancing window : 3
Probe suppression mode                  : Disabled
Probe suppression validity window       : 100 s
Probe suppression aggregate window      : 200 ms
Probe suppression transition aggressiveness : 3
Probe suppression hysteresis           : -6 dBm

WLAN Configuration Information

----- show wireless client calls active -----

----- show wireless client calls rejected -----

----- show wireless client sleeping-client -----

Total number of sleeping-client entries: 0

```

----- show wireless client probing -----

----- show wireless client ap dot11 24ghz -----

----- show wireless client ap dot11 5ghz -----

----- show wireless pmk-cache -----

Number of PMK caches in total : 0

| Type | Station | Entry Lifetime | VLAN Override | IP Override |
|------------------|---------|----------------|---------------|-------------|
| Audit-Session-Id | | | | |

----- show wireless exclusionlist -----

----- show wireless country configured -----

Configured Country..... US - United States
 Configured Country Codes
 US - United States 802.11a Indoor/ 802.11b Indoor/ 802.11g Indoor

----- show wireless tag rf summary -----

Number of RF Tags: 1

| RF tag name | Description |
|----------------|----------------|
| default-rf-tag | default RF tag |

----- show platform software wireless-client chassis active R0 statistics -----

| Client Counters | (Success/Failure) |
|-----------------|-------------------|
| Create | 0/0 |
| Delete | 0/0 |
| Modify | 0/0 |
| Switch 1: | |
| OM Create | 0/0 |
| OM Delete | 0/0 |

show tech-support wireless client

```

NACK Notify          0/0
  Create Failure     0
  Modify Failure     0
  Delete Failure     0

```

```

----- show platform software wireless-client chassis active F0 statistics
-----

```

```

Client Counters      (Success/Failure)
-----
Create                0/0
Delete                0/0
HW Create             0/0
HW Modify             0/0
HW Delete             0/0
Create Ack            0/0
Modify Ack            0/0
Delete Ack           0/0
NACK Notify           0/0

```

```

----- show platform hardware chassis active qfp feature wireless wlclient
cpp-client summary -----

```

```

----- show platform hardware chassis active qfp feature wireless wlclient
datapath summary -----

```

```

Vlan  pal_if_hdl  mac          Input Uidb Output Uidb
-----

```


show tech-support wireless datapath

To print the data related to CPP datapath, use the **show tech-support wireless datapath** command in privileged EXEC mode.

show tech-support wireless datapath

| | | |
|---------------------------|--|------------------------------|
| 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 | <p>This command is available only on the platforms that have CPP datapath architecture, such as Cisco vEWLC, Cisco 9540 WLC, and Cisco 9880 WLC.</p> <p>The output of the following commands are displayed as part of show tech-support wireless datapath command:</p> <ul style="list-style-type: none"> • show platform hardware chassis active qfp feature wireless bssid summary • show platform hardware chassis active qfp feature wireless capwap cpp-client statistics • show platform hardware chassis active qfp feature wireless capwap cpp-client summary • show platform hardware chassis active qfp feature wireless capwap datapath statistics drop • show platform hardware chassis active qfp feature wireless capwap datapath statistics fragmentation • show platform hardware chassis active qfp feature wireless capwap datapath statistics reassembly • show platform hardware chassis active qfp feature wireless capwap datapath summary • show platform hardware chassis active qfp feature wireless dtls cpp-client statistics • show platform hardware chassis active qfp feature wireless dtls cpp-client summary • show platform hardware chassis active qfp feature wireless dtls datapath statistics • show platform hardware chassis active qfp feature wireless dtls datapath summary • show platform hardware chassis active qfp feature wireless et-analytics eta-pending-client-tree • show platform hardware chassis active qfp feature wireless et-analytics statistics • show platform hardware chassis active qfp feature wireless fqdn-filter summary • show platform hardware chassis active qfp feature wireless halo statistics • show platform hardware chassis active qfp feature wireless ipsg cpp-client statistics | |

- show platform hardware chassis active qfp feature wireless ipsg cpp-client table ipv4 all
- show platform hardware chassis active qfp feature wireless ipsg cpp-client table ipv6 all
- show platform hardware chassis active qfp feature wireless ipsg datapath statistics global
- show platform hardware chassis active qfp feature wireless ipsg datapath table ipv4 all
- show platform hardware chassis active qfp feature wireless ipsg datapath table ipv6 all
- show platform hardware chassis active qfp feature wireless mgmt-intf cpp-client summary
- show platform hardware chassis active qfp feature wireless mgmt-intf datapath summary
- show platform hardware chassis active qfp feature wireless punt statistics
- show platform hardware chassis active qfp feature wireless wlan summary
- show platform hardware chassis active qfp feature wireless wlclient cpp-client statistics
- show platform hardware chassis active qfp feature wireless wlclient cpp-client summary
- show platform hardware chassis active qfp feature wireless wlclient datapath statistic drop
- show platform hardware chassis active qfp feature wireless wlclient datapath summary
- show platform hardware chassis active qfp feature wireless wlclient datapath table dataglean all
- show platform hardware chassis active qfp infrastructure punt statistics type per-cause
- show platform hardware chassis active qfp statistics drop
- show platform software bssid chassis active F0
- show platform software bssid chassis active F0 statistics
- show platform software capwap chassis active F0
- show platform software capwap chassis active F0 statistics
- show platform software dtls chassis active F0
- show platform software dtls chassis active F0 statistics
- show platform software wireless-client chassis active F0
- show platform software wireless-client chassis active F0 statistics
- show platform software wlan chassis active F0

In the presence of standby node, the following datapath commands are also displayed:

- show platform hardware chassis standby qfp feature wireless bssid summary
- show platform hardware chassis standby qfp feature wireless capwap cpp-client statistics
- show platform hardware chassis standby qfp feature wireless capwap cpp-client summary
- show platform hardware chassis standby qfp feature wireless capwap datapath statistics drop
- show platform hardware chassis standby qfp feature wireless capwap datapath statistics fragmentation
- show platform hardware chassis standby qfp feature wireless capwap datapath statistics reassembly

- show platform hardware chassis standby qfp feature wireless capwap datapath summary
- show platform hardware chassis standby qfp feature wireless dtls cpp-client statistics
- show platform hardware chassis standby qfp feature wireless dtls cpp-client summary
- show platform hardware chassis standby qfp feature wireless dtls datapath statistics
- show platform hardware chassis standby qfp feature wireless dtls datapath summary
- show platform hardware chassis standby qfp feature wireless halo statistics
- show platform hardware chassis standby qfp feature wireless ipsg cpp-client statistics
- show platform hardware chassis standby qfp feature wireless ipsg cpp-client table ipv4 all
- show platform hardware chassis standby qfp feature wireless ipsg cpp-client table ipv6 all
- show platform hardware chassis standby qfp feature wireless ipsg datapath statistics global
- show platform hardware chassis standby qfp feature wireless ipsg datapath table ipv4 all
- show platform hardware chassis standby qfp feature wireless ipsg datapath table ipv6 all
- show platform hardware chassis standby qfp feature wireless mgmt-intf cpp-client summary
- show platform hardware chassis standby qfp feature wireless mgmt-intf datapath summary
- show platform hardware chassis standby qfp feature wireless punt statistics
- show platform hardware chassis standby qfp feature wireless wlan summary
- show platform hardware chassis standby qfp feature wireless wlclient cpp-client statistics
- show platform hardware chassis standby qfp feature wireless wlclient cpp-client summary
- show platform hardware chassis standby qfp feature wireless wlclient datapath statistic drop
- show platform hardware chassis standby qfp feature wireless wlclient datapath summary
- show platform hardware chassis standby qfp feature wireless wlclient datapath table dataglean all
- show platform hardware chassis standby qfp statistics drop
- show platform software bssid chassis standby F0
- show platform software bssid chassis standby F0 statistics
- show platform software capwap chassis standby F0
- show platform software capwap chassis standby F0 statistics
- show platform software dtls chassis standby F0
- show platform software dtls chassis standby F0 statistics
- show platform software wireless-client chassis standby F0
- show platform software wireless-client chassis standby F0 statistics
- show platform software wlan chassis standby F0

Example

The following is sample output from the **show tech-support wireless datapath** command

```
Device# show tech-support wireless datapath
```

```
----- show platform hardware chassis active qfp statistics drop
-----
```

| Global Drop Stats | Packets | Octets |
|---------------------------|---------|-----------|
| Disabled | 22230 | 2045194 |
| InvL2Hdr | 4765368 | 744492240 |
| Ipv4NoAdj | 6 | 736 |
| Ipv4NoRoute | 18 | 2358 |
| Ipv6mcNoRoute | 3 | 270 |
| SWPortDrop | 14432 | 2886027 |
| SWPortSrcFilter | 53265 | 53992718 |
| SWPortStpState | 42041 | 3269790 |
| SWPortVlanNotCfg | 5515542 | 674079804 |
| SwitchL2m | 78 | 10062 |
| SwitchL2mIGMP | 18866 | 1283348 |
| SwitchL2mUnconfigWireless | 78 | 11622 |
| WlsCapwapNoTunnel | 3 | 627 |

```
----- show platform hardware chassis active qfp feature wireless punt statistics
-----
```

```
CPP Wireless Punt stats:
```

| App Tag | Packet Count |
|------------------------------------|--------------|
| CAPWAP_PKT_TYPE_DOT11_PROBE_REQ | 0 |
| CAPWAP_PKT_TYPE_DOT11_MGMT | 56 |
| CAPWAP_PKT_TYPE_DOT11_IAPP | 22177 |
| CAPWAP_PKT_TYPE_DOT11_RFID | 0 |
| CAPWAP_PKT_TYPE_DOT11_RRM | 0 |
| CAPWAP_PKT_TYPE_DOT11_DOT1X | 0 |
| CAPWAP_PKT_TYPE_CAPWAP_KEEPALIVE | 0 |
| CAPWAP_PKT_TYPE_MOBILITY_KEEPALIVE | 0 |
| CAPWAP_PKT_TYPE_CAPWAP_CNTRL | 303661 |
| CAPWAP_PKT_TYPE_CAPWAP_DATA | 0 |
| CAPWAP_PKT_TYPE_MOBILITY_CNTRL | 0 |
| WLS_SMD_WEBAUTH | 0 |
| SISF_PKT_TYPE_ARP | 303 |
| SISF_PKT_TYPE_DHCP | 282 |
| SISF_PKT_TYPE_DHCP6 | 0 |
| SISF_PKT_TYPE_IPV6_ND | 0 |
| SISF_PKT_TYPE_DATA_GLEAN | 0 |
| SISF_PKT_TYPE_DATA_GLEAN_V6 | 0 |
| SISF_PKT_TYPE_DHCP_RELAY | 0 |
| CAPWAP_PKT_TYPE_CAPWAP_RESERVED | 0 |

```
----- show platform hardware chassis active qfp infrastructure punt statistics
type per-cause -----
```

```
Global Per Cause Statistics
```

Number of punt causes = 136

Per Punt Cause Statistics

| Counter ID | Punt Cause Name | Packets Received | Packets Transmitted |
|------------|---------------------------------|------------------|---------------------|
| 000 | Reserved | 0 | 0 |
| 001 | MPLS ICMP Can't Fragment | 0 | 0 |
| 002 | IPv4 Options | 0 | 0 |
| 003 | Layer2 control and legacy | 0 | 0 |
| 004 | PPP Control | 0 | 0 |
| 005 | CLNS IS-IS Control | 0 | 0 |
| 006 | HDLC keepalives | 0 | 0 |
| 007 | ARP request or response | 2687 | 2687 |
| 008 | Reverse ARP request or response | 0 | 0 |
| 009 | Frame-relay LMI Control | 0 | 0 |
| 010 | Incomplete adjacency | 0 | 0 |
| 011 | For-us data | 0 | 0 |
| 012 | Mcast Directly Connected Source | 0 | 0 |
| 013 | Mcast IPv4 Options data packet | 0 | 0 |
| 014 | Skip egress processing | 0 | 0 |
| 015 | MPLS TTL expired | 0 | 0 |
| 016 | MPLS Reserved label (ie: 0-15) | 0 | 0 |
| 017 | IPv6 Bad hop limit | 0 | 0 |
| 018 | IPV6 Hop-by-hop Options | 0 | 0 |
| 019 | Mcast Internal Copy | 0 | 0 |
| 020 | Generic QFP generated packet | 0 | 0 |
| 021 | RP<->QFP keepalive | 46691 | 46691 |
| 022 | QFP Fwall generated packet | 0 | 0 |
| 023 | Mcast IGMP Unroutable | 0 | 0 |
| 024 | Glean adjacency | 2557 | 2556 |
| 025 | Mcast PIM signaling | 0 | 0 |
| 026 | QFP ICMP generated packet | 0 | 0 |
| 027 | Subscriber session control | 0 | 0 |

| | | | |
|-----|--|---|---|
| 028 | Subscriber data switching back | 0 | 0 |
| 029 | RP handled ICMP | 0 | 0 |
| 030 | RP injected For-us data | 0 | 0 |
| 031 | Punt adjacency | 0 | 0 |
| 032 | SBC RTP DTMF | 0 | 0 |
| 033 | Pseudowire VCCV control channel | 0 | 0 |
| 034 | Generic QFP generated packet (keep GPM) | 0 | 0 |
| 035 | Ethernet slow protocol (ie: LACP, OAM) | 0 | 0 |
| 036 | Ethernet OAM Loopback | 0 | 0 |
| 037 | UNUSED | 0 | 0 |
| 038 | SPA IPC packet | 0 | 0 |
| 039 | Punt and replicate | 0 | 0 |
| 040 | PPPoE control | 0 | 0 |
| 041 | PPPoE session | 0 | 0 |
| 042 | L2TP control | 0 | 0 |
| 043 | IP Subscriber control (ie: FSOL, keepali | 0 | 0 |
| 044 | L2TP session | 0 | 0 |
| 045 | BFD control | 0 | 0 |
| 046 | MVPN non-RPF signaling packet | 0 | 0 |
| 047 | MVPN PIM signalling packet | 0 | 0 |
| 048 | Mcast punt to RP | 0 | 0 |
| 049 | SBC generated packet | 0 | 0 |
| 050 | IPv6 packet | 0 | 0 |
| 051 | DMVPN NHRP redirect | 0 | 0 |
| 052 | PFR monitored prefix logging | 0 | 0 |
| 053 | PFR top talkers logging | 0 | 0 |
| 054 | PFR top talkers application logging | 0 | 0 |
| 055 | For-us control | 0 | 0 |
| 056 | RP injected for-us control | 0 | 0 |
| 057 | QFP VTCP generated packet | 0 | 0 |
| 058 | Layer2 bridge domain data packet | 0 | 0 |
| 059 | QFP Stile generated packet | 0 | 0 |

| | | | |
|-----|--|--------|--------|
| 060 | IP subnet or broadcast packet | 167 | 167 |
| 061 | Ethernet CFM packet | 0 | 0 |
| 062 | Ethernet CFM notify packet | 0 | 0 |
| 063 | LISP LSB NOTIFICATION | 0 | 0 |
| 064 | Service Engine packet | 0 | 0 |
| 065 | L2BD Control packet from FIA | 0 | 0 |
| 066 | L2BD Control Message from CPP | 0 | 0 |
| 067 | MFR_LIP_CONTROL | 0 | 0 |
| 068 | Media Monitoring record punted from CPP | 0 | 0 |
| 069 | OTV Control packet | 0 | 0 |
| 070 | OTV ARP packet | 0 | 0 |
| 071 | REP control | 0 | 0 |
| 072 | IP MTU EXCEPTION | 0 | 0 |
| 073 | STP BPDU's | 186832 | 186832 |
| 074 | ACL log | 0 | 0 |
| 075 | EPC | 0 | 0 |
| 076 | Lisp Dynamic eid | 0 | 0 |
| 077 | L2 Control packet | 122389 | 122389 |
| 078 | WAAS CPP to CPP punt | 0 | 0 |
| 079 | dhcp snoop | 0 | 0 |
| 080 | Metric Mediation Agent record punted fro | 0 | 0 |
| 081 | IPv6 DMVPN NHRP redirect | 0 | 0 |
| 082 | Ethernet CFM packet from core | 0 | 0 |
| 083 | Ethernet CFM punt fwd packet | 0 | 0 |
| 084 | PTP punt fwd packet | 0 | 0 |
| 085 | ISDN D-Channel raw packet | 0 | 0 |
| 086 | Service controller SCG punt pkt | 0 | 0 |
| 087 | IPv6 FHS SG dropped packet | 0 | 0 |
| 088 | IPv6 FHS Data glean packet | 0 | 0 |
| 089 | SBC DSP pkts | 0 | 0 |
| 090 | Raw Socket Data packet | 0 | 0 |
| 091 | SSLVPN session control | 0 | 0 |

| | | | |
|-----|--|-------|-------|
| 092 | ICMP unreachable for ACL denied packets | 0 | 0 |
| 093 | CENT Smart Probe packet | 0 | 0 |
| 094 | AppNav vPATH pktless API generated pkt | 0 | 0 |
| 095 | Autonomic Network Channel Discovery pack | 0 | 0 |
| 096 | Layer2 control protocols | 0 | 0 |
| 097 | Packets to LFTS | 22177 | 22177 |
| 098 | VLAN Auto Sense FSOL | 0 | 0 |
| 099 | ZTP Discovery packet | 0 | 0 |
| 100 | cable arp filter | 0 | 0 |
| 101 | Cable L3 mobility | 0 | 0 |
| 102 | Source Verify inconclusive | 0 | 0 |
| 103 | cable modem pre reg | 0 | 0 |
| 104 | mpls receive adj | 0 | 0 |
| 105 | MKA EAPoL packet | 0 | 0 |
| 106 | ICMP Unreachable | 0 | 0 |
| 107 | Cable DHCP | 0 | 0 |
| 108 | Snooping packet | 0 | 0 |
| 109 | snoop packets | 0 | 0 |
| 110 | msg Indicating ppp intf assigned ip addr | 0 | 0 |
| 111 | msg indicating there is another common h | 0 | 0 |
| 112 | QoS CAC Flow Report | 0 | 0 |
| 113 | Active identity | 0 | 0 |
| 114 | BGP Overlay Tunnel packet | 0 | 0 |
| 115 | Lisp gsmr enabled | 0 | 0 |
| 116 | Async TS | 0 | 0 |
| 117 | Metric Mediation Agent Packet | 0 | 0 |
| 118 | Cable DHCPV6 Solicit | 0 | 0 |
| 119 | Cable DHCPV6 Request | 0 | 0 |
| 120 | SBC RTP FWD DTMF | 0 | 0 |
| 121 | Path Manager | 0 | 0 |
| 122 | L2 LISP VXLAN | 0 | 0 |
| 123 | dialer-list | 0 | 0 |

| | | | |
|-----|--------------------------------|--------|--------|
| 124 | Dialer update time | 0 | 0 |
| 125 | Cable RPHY CTRL | 0 | 0 |
| 126 | OpenFlow SDN | 0 | 0 |
| 127 | Path Manager TTL expired | 0 | 0 |
| 128 | L3 PTP message | 0 | 0 |
| 129 | wls 802.11 Packets to LFTS | 56 | 56 |
| 130 | wls CAPWAP Packets to LFTS | 303661 | 303661 |
| 131 | wls MOBILITY Packets to LFTS | 0 | 0 |
| 132 | wls SISF Packets to LFTS | 585 | 585 |
| 133 | cable DHCPv6 subscriber-side | 0 | 0 |
| 134 | cable DHCPv4 subscriber-side | 0 | 0 |
| 135 | cable DHCPv4 sub-side disc/req | 0 | 0 |

Number of inject causes = 49

Per Inject Cause Statistics

| Counter ID | Inject Cause Name | Packets Received | Packets Transmitted |
|------------|------------------------------------|------------------|---------------------|
| 000 | RESERVED | 0 | 0 |
| 001 | L2 control/legacy | 3115 | 3115 |
| 002 | QFP destination lookup | 0 | 0 |
| 003 | QFP IPv4/v6 nexthop lookup | 0 | 0 |
| 004 | QFP generated packet | 0 | 0 |
| 005 | QFP <->RP keepalive | 46691 | 0 |
| 006 | QFP Fwall generated packet | 0 | 0 |
| 007 | QFP adjacency-id lookup | 0 | 0 |
| 008 | Mcast specific inject packet | 0 | 0 |
| 009 | QFP ICMP generated packet | 0 | 0 |
| 010 | QFP/RP->QFP Subscriber data packet | 0 | 0 |
| 011 | SBC DTMF | 0 | 0 |
| 012 | ARP request or response | 3637 | 3637 |
| 013 | Ethernet OAM loopback packet | 0 | 0 |

show tech-support wireless datapath

| | | | |
|-----|--|--------|--------|
| 014 | UNUSED | 0 | 0 |
| 015 | PPPoE discovery packet | 0 | 0 |
| 016 | PPPoE session packet | 0 | 0 |
| 017 | QFP inject for pp_index lookup | 0 | 0 |
| 018 | QFP inject replicate | 0 | 0 |
| 019 | QFP inject PIT lookup | 0 | 0 |
| 020 | SBC generated packets | 0 | 0 |
| 021 | QFP VTCP generated packet | 0 | 0 |
| 022 | QFP Stile generated packet | 0 | 0 |
| 023 | Service Engine generated packet | 0 | 0 |
| 024 | Layer2 frame to EFP | 0 | 0 |
| 025 | Layer2 frame to BD | 0 | 0 |
| 026 | QFP Asym Routing redirected pkt | 0 | 0 |
| 027 | Compressed packet from WAAS | 0 | 0 |
| 028 | Media (e.g. voice) associated with a ses | 0 | 0 |
| 029 | service controller scg packet | 0 | 0 |
| 030 | Packet for 14 port Serial IM | 0 | 0 |
| 031 | Subscriber generated TCP reset packet | 0 | 0 |
| 032 | Layer2 frame to INPUT EFP | 0 | 0 |
| 033 | SSLVPN inject control | 0 | 0 |
| 034 | injected packet from UTD SP | 0 | 0 |
| 035 | injected packet from DPSS SN | 0 | 0 |
| 036 | injected packet by AppNav vPath | 0 | 0 |
| 037 | Uncompressed packet from WAAS | 0 | 0 |
| 038 | Autonomic Network Channel Discovery pack | 0 | 0 |
| 039 | Cable Bundle Flood Inject | 0 | 0 |
| 040 | Cable L2 unicast inject | 0 | 0 |
| 041 | downstream jib packet | 0 | 0 |
| 042 | switch port layer 2 control packet | 6254 | 6253 |
| 043 | Applications Injecting Pkts using LFTS | 303874 | 303269 |
| 044 | Enhanced ping and traceroute | 0 | 0 |
| 045 | Applications Injecting packets with SGT | 0 | 0 |

```

046      CoPP packets from EPC_WS          0          0
047      Async TS                          0          0
048      Layer2 frame to VLAN              0          0
    
```

----- show platform hardware chassis active qfp feature wireless mgmt-intf
cpp-client summary -----

Wireless Management Interface Info

```

CPP IF_H  VLAN  MAC Address
-----
0XF      78   001e.1405.2bff
    
```

----- show platform hardware chassis active qfp feature wireless mgmt-intf
datapath summary -----

Wireless Management Interface Info

```

IF_H      VLAN  MAC Address
-----
0xF      78   001e.1405.2bff
    
```

----- show platform software wlan chassis active F0 -----

| WLAN Interface ID | WLAN ID | WLAN Name | AOM ID | Status |
|-------------------|---------|-----------|--------|--------|
| 0xf0400001 | 1 | att | 275 | Done |
| 0xf0400002 | 2 | verizon | 292 | Done |

----- show platform hardware chassis active qfp feature wireless wlan summary

CPP Wlan Database Summary

Total number of wlan interfaces : 2

| if_name ssid | cpp_if_hdl | pal_if_hdl | in_uidb | out_uidb |
|---------------------------------|------------|------------|---------|----------|
| WLAN-IF-0x00f0400001 att | 0X74 | 0XF0400001 | 0X1768E | 0X1768C |
| WLAN-IF-0x00f0400002 verizon | 0X78 | 0XF0400002 | 0X1768A | 0X17688 |

----- show platform software bssid chassis active F0 statistics

Bssid Counters (Success/Failure)

```

-----
Create          0/0
Delete          0/0
HW Create       0/0
    
```

show tech-support wireless datapath

```

HW Modify          0/0
HW Delete          0/0
Create Ack         0/0
Modify Ack         0/0
Delete Ack        0/0
Nack Notify       0/0

```

```
----- show platform software bssid chassis active F0 -----
```

```
----- show platform hardware chassis active qfp feature wireless bssid summary
-----
```

```
----- show platform software capwap chassis active F0 statistics
-----
```

```

Capwap Counters   (Success/Failure)
-----
Create            424/0
Delete            420/0
HW Create         424/0
HW Modify         0/0
HW Delete        420/0
Create Ack       424/0
Modify Ack       0/0
Delete Ack      420/0
Ack Ack Notify   0/0
Ack Nack Notify 0/0
Nack Notify     0/0

```

```
----- show platform software capwap chassis active F0 -----
```

| Tunnel ID | AP MAC | Type | IP | Port | AOM ID | Status |
|------------|----------------|---------------|-----------|-------|--------|--------|
| 0x90000042 | 00a8.2200.0200 | Data | 78.1.50.1 | 52345 | 3271 | Done |
| 0xa0000002 | 0000.0000.0000 | Mobility Data | 78.1.1.23 | 16667 | 1426 | Done |
| 0xa0000003 | 0000.0000.0000 | Mobility Data | 78.1.1.24 | 16667 | 1427 | Done |
| 0xa0000004 | 0000.0000.0000 | Mobility Data | 78.1.1.25 | 16667 | 1428 | Done |

```
----- show platform hardware chassis active qfp feature wireless capwap
cpp-client statistics -----
```

```

CAPWAP cpp-client plumbing statistics
Number Msg in = ack + nak + ack fail + nak fail + errors

Counter                                     Value
-----
Create from fp                             424

```

```

Modify from fp                0
Delete from fp                420
Create ack to fp              424
Create ack fail to fp         0
Create nack to fp             0
Create nack fail to fp        0
Modify ack to fp              0
Modify ack fail to fp         0
Modify nack to fp             0
Modify nack fail to fp        0
Delete ack to fp              420
Delete ack fail to fp         0
Delete nack to fp             0
Delete nak fail to fp         0
    
```

----- show platform hardware chassis active qfp feature wireless capwap
cpp-client summary -----

| cpp_if_hdl Tun Type | pal_if_hdl | AP MAC | Src IP | Dst IP | Dst Port |
|------------------------|------------|----------------|----------|-----------|----------|
| 0X108 DATA | 0X90000042 | 00a8.2200.0200 | 78.1.1.7 | 78.1.50.1 | 52345 |
| 0X10B MOBILITY | 0XA0000002 | 0000.0000.0000 | 78.1.1.7 | 78.1.1.23 | 16667 |
| 0X10C MOBILITY | 0XA0000003 | 0000.0000.0000 | 78.1.1.7 | 78.1.1.24 | 16667 |
| 0X10D MOBILITY | 0XA0000004 | 0000.0000.0000 | 78.1.1.7 | 78.1.1.25 | 16667 |

----- show platform hardware chassis active qfp feature wireless capwap datapath
summary -----

| Vrf | Src Port | Dst IP | Dsp Port | Input Uidb | Output Uidb | Instance Id |
|-----|----------|-----------|----------|------------|-------------|-------------|
| 0 | 16667 | 78.1.1.25 | 16667 | 95733 | 95731 | 0 |
| 0 | 5247 | 78.1.50.1 | 52345 | 95738 | 95736 | 3 |
| 0 | 16667 | 78.1.1.24 | 16667 | 95734 | 95732 | 0 |
| 0 | 16667 | 78.1.1.23 | 16667 | 95735 | 95733 | 0 |

----- show platform hardware chassis active qfp feature wireless capwap datapath
statistics drop -----

| Drop Cause Octets | Packets |
|---|---------|
| Wls Capwap unsupported link type Error 0 | 0 |
| Wls Capwap invalid tunnel Error 0 | 0 |
| Wls Capwap input config missing Error 0 | 0 |
| Wls Capwap invalid TPID Error 0 | 0 |
| Wls Capwap ingress parsing Error 0 | 0 |

show tech-support wireless datapath

```

Wls Capwap invalid FC subtype Error          0
      0
Wls Capwap SNAP Invalid HLEN Error          0
      0
Wls Client V6 Max Address Error             0
      0

```

```

----- show platform hardware chassis active qfp feature wireless capwap datapath
statistics fragmentation -----

```

CPP Wireless Fragmentation stats:

| Description | Packet Count | Octet Count |
|--------------------------------------|--------------|-------------|
| ----- | ----- | ----- |
| Capwap Packets to be Fragmented (RX) | 0 | 0 |
| Capwap Fragments to be Recycled | 0 | 0 |
| Capwap Fragments Recycled (TX) | 0 | 0 |
| Error: Original Packet Too Big | 0 | 0 |
| Error: CAPWAP MTU Not Valid | 0 | 0 |
| Error: Recycle Queue Full | 0 | 0 |
| Error: Recycle Queue Not Valid | 0 | 0 |
| Error: GPM Memory Init Failure | 0 | 0 |
| Error: Multipass Requeue Failure | 0 | 0 |

```

----- show platform hardware chassis active qfp feature wireless capwap datapath
statistics reassembly -----

```

CPP Wireless Reassembly Memory stats:

| Description | Count |
|---------------------------|--------|
| ----- | ----- |
| Free info chunk | 32768 |
| Allocated info chunks | 32768 |
| Free fragment chunks | 131072 |
| Allocated fragment chunks | 131072 |

CPP Wireless Reassembly Packet stats: (outstanding pkt_cnt 0)

| Description | Packet Count | Octet Count |
|-------------------------------------|--------------|-------------|
| ----- | ----- | ----- |
| Capwap Reassembled Packets | 0 | 0 |
| Capwap Fragments Received | 0 | 0 |
| Capwap Fragments Consumed (Saved) | 0 | 0 |
| Capwap Fragments Dropped | 0 | 0 |
| Capwap Reassembly Timeouts | 0 | 0 |
| Error - Early-drop fragments | 0 | 0 |
| Error - Invalid packet size | 0 | 0 |
| Error - Fragment size too big | 0 | 0 |
| Error - Too many fragments | 0 | 0 |
| Error - Overlap offset fragments | 0 | 0 |
| Error - Duplicated fragments | 0 | 0 |
| Error - Allocate info chunk memory | 0 | 0 |
| Error - Allocate frag chunk memory | 0 | 0 |
| Error - Hash bucket threshold | 0 | 0 |
| Error - Cannot save and gather pkts | 0 | 0 |
| Error - Get recycle reass_info NULL | 0 | 0 |
| Error - BQS memory alloc NULL | 0 | 0 |
| Error - BQS memory free NULL | 0 | 0 |

```

DEBUG - # of lock sync aquired          2          2
DEBUG - # of lock released              2          2
DEBUG - CPP_CW_BQS_MX_ALLOC #           0          0
DEBUG - CPP_CW_BQS_MX_FREE #            0          0
DEBUG - CPP_REASS_INFO_ALLOC #          0          0
DEBUG - CPP_REASS_INFO_FREE #           0          0
DEBUG - CPP_REASS_FRAG_ALLOC #          0          0
DEBUG - CPP_REASS_FRAG_FREE #           0          0
    
```

----- show platform software dtls chassis active F0 statistics -----

```

DTLS Counters      (Success/Failure)
-----
Create              847/0
Delete              424/0
HW Create           425/0
HW Modify           422/0
HW Delete           424/0
Create Ack          425/0
Modify Ack          422/0
Delete Ack          424/0
Ack Ack Notify     1271/0
Ack Nack Notify    0/0
Nack Notify        0/0
HA Seq GET         782/0
HA Seq SET         0/0
HA Seq Crypto GET  1542/0
HA Seq Crypto SET  0/0
HA Seq Crypto Callback 1542/0

HA Seq last Responded 0
HA Seq Pending        0
HA Seq Outstanding cb 0
Total DTLS CTX count  1
    
```

----- show platform software dtls chassis active F0 -----

Forwarding Manager DTLS Session Summary

| Session ID | Type | Peer IP | Port | AOM ID | Status |
|--------------------|------------|-----------|-------|--------|--------|
| 0x0300000000000001 | AP Control | 78.1.50.1 | 52345 | 3270 | Done |

----- show platform hardware chassis active qfp feature wireless dtls cpp-client statistics -----

```

DTLS cpp-client plumbing statistics
Number Msg in = ack + nak + ack fail + nak fail + errors

Counter                      Value
-----
Create from fp                425
Modify from fp                422
Delete from fp                424
    
```

show tech-support wireless datapath

```

Create ack to fp          425
Create ack fail to fp    0
Create nack to fp        0
Create nack fail to fp   0
Modify ack to fp         422
Modify ack fail to fp    0
Modify nack to fp        0
Modify nack fail to fp   0
Delete ack to fp         424
Delete ack fail to fp    0
Delete nack to fp        0
Delete nak fail to fp    0
    
```

----- show platform hardware chassis active qfp feature wireless dtls cpp-client summary -----

| Session ID | CDH Handle | Session Type | Parent if-h | Instance id |
|--------------------|--------------------|--------------|-------------|-------------|
| 0x0300000000000001 | 0x00000000D902D9E0 | AP Control | 0 | 3 |

----- show platform hardware chassis active qfp feature wireless dtls datapath summary -----

| Src IP | Dst IP | Src Port | Dst Port | Crypto HDL | Instance Id |
|----------|-----------|----------|----------|------------|-------------|
| 78.1.1.7 | 78.1.50.1 | 5246 | 52345 | 0xd902d9e0 | 3 |

----- show platform hardware chassis active qfp feature wireless dtls datapath statistics -----

CPP Wireless DTLS Feature Stats

| Description | Packet Count | Octet Count |
|--------------------------------------|--------------|-------------|
| DTLS Packets To Encrypt | 286494 | 8860778 |
| DTLS Packets Encrypted | 286494 | 35681366 |
| DTLS Packets To Decrypt | 286734 | 41001830 |
| DTLS Packets Decrypted | 286734 | 33401602 |
| Skip Encryption - Handshake | 0 | 0 |
| Skip Encryption - Not AppData | 0 | 0 |
| Skip Encryption - No Hash Entry | 0 | 0 |
| Skip Encryption - No Crypto Handle | 0 | 0 |
| Skip Encryption - No DTLS header | 563 | 76419 |
| Skip Encryption - Requested by RP | 16234 | 5042852 |
| Skip Decryption - Handshake | 0 | 0 |
| Skip Decryption - Not AppData | 2949 | 996248 |
| Skip Decryption - No Hash Entry | 447 | 56474 |
| Skip Decryption - No Crypto Handle | 13024 | 3626640 |
| Skip Decryption - No DTLS header | 507 | 116600 |
| Skip Decryption - Multiple Records | 0 | 0 |
| Error - Encrypt Invalid Length | 0 | 0 |
| Error - Encrypt Header Restore | 0 | 0 |
| Error - DataEncrypt No Crypto Handle | 0 | 0 |
| Error - DataEncrypt Header Restore | 0 | 0 |
| Error - Decrypt Invalid Length | 0 | 0 |
| Error - Decrypt Header Restore | 0 | 0 |
| Error - DataDecrypt Zero Epoch | 0 | 0 |


```
Error - DataDecrypt No Hash Entry          0          0
Error - DataDecrypt No Crypto Handle       0          0
Error - DataDecrypt Header Restore         0          0
```

----- show platform software wireless-client chassis active F0 statistics -----

Client Counters (Success/Failure)

```
-----
Create          112/0
Delete          55/0
HW Create       56/0
HW Modify       56/0
HW Delete       55/0
Create Ack      56/0
Modify Ack      56/0
Delete Ack      55/0
NACK Notify     0/0
```

----- show platform software wireless-client chassis active F0 -----

| ID | MAC Address | WLAN | Client State | AOM ID | Status |
|------------|----------------|------|--------------|--------|--------|
| 0xa0000001 | 0028.b122.0001 | 1 | Run | 3272 | Done |

----- show platform hardware chassis active qfp feature wireless wlclient cpp-client statistics -----

Wlclient cpp-client plumbing statistics
 Number Msg in = ack + nak + ack fail + nak fail + errors

| Counter | Value |
|------------------------|-------|
| Create from fp | 56 |
| Modify from fp | 56 |
| Delete from fp | 55 |
| Create ack to fp | 56 |
| Create ack fail to fp | 0 |
| Create nack to fp | 0 |
| Create nack fail to fp | 0 |
| Modify ack to fp | 56 |
| Modify ack fail to fp | 0 |
| Modify nack to fp | 0 |
| Modify nack fail to fp | 0 |
| Delete ack to fp | 55 |
| Delete ack fail to fp | 0 |
| Delete nack to fp | 0 |
| Delete nak fail to fp | 0 |

----- show platform hardware chassis active qfp feature wireless wlclient cpp-client summary -----

Auth State Abbreviations:
 UK - UNKNOWN IP - LEARN IP
 L3 - L3 AUTH RN - RUN

show tech-support wireless datapath

```

IV - INVALID
Mobility State Abbreviations:
  UK - UNKNOWN  IN - INIT
  LC - LOCAL    AN - ANCHOR
  FR - FOREIGN  MT - MTE
  IV - INVALID
CPP IF_H      DPIDX      MAC Address      VLAN  AS  MS              WLAN
POA
-----
0X102      0XA0000001  0028.b122.0001  177  RN  LC              att
0x90000042

```

----- show platform hardware chassis active qfp feature wireless wlclient datapath summary -----

| Vlan | pal_if_hdl | mac | Input Uidb | Output Uidb |
|------|------------|----------------|------------|-------------|
| 177 | 0xa0000001 | 0028.b122.0001 | 95744 | 95742 |

----- show platform hardware chassis active qfp feature wireless wlclient datapath statistic drop -----

| Drop Cause | Octets | Packets |
|--|--------|---------|
| Wls Client V6 Max Address Error | 0 | 0 |
| Wls Client IPGlean Counter Index Error | 0 | 0 |
| Wls Client IPGlean Counter Unchanged Error | 0 | 0 |
| Wls Client IPGlean alloc no memory Error | 0 | 0 |
| Wls Client invalid punt packet error | 0 | 0 |
| Wls Client input subblock missing error | 0 | 0 |
| Wls Client input config missing | 0 | 0 |
| Wls Client global mac address fetch error | 0 | 0 |
| Wls Client header add error | 0 | 0 |
| Wls Client IP entry theft error | 0 | 0 |
| Wls Client IPSG input subblock missing error | 0 | 0 |
| Wls Client DOT1Q Hdr add anchor error | 0 | 0 |
| Wls Client DOT1Q Hdr add anchor avc error | 0 | 0 |
| Wls Client Guest Foreign Multicast error | 0 | 0 |

----- show platform hardware chassis active qfp feature wireless wlclient datapath table dataglean all -----

CPP Wireless IPv6 Data Gleaning Table:

| IP Address | VLAN | uIDB | Interface |
|------------|------|------|-----------|
|------------|------|------|-----------|

----- show platform hardware chassis active qfp feature wireless ipsg cpp-client statistics -----

CPP Wireless IPSG CPP-client Statistics

| Counter | Value |
|-----------------------------|-------|
| Total IPv4 Address Count | 1 |
| Total IPv6 Address Count | 0 |
| IPv4 Entry Add Success | 56 |
| IPv4 Entry Add Fail | 0 |
| IPv4 Entry Delete Success | 55 |
| IPv4 Entry Delete Fail | 0 |
| IPv6 Entry Add Success | 0 |
| IPv6 Entry Add Fail | 0 |
| IPv6 Entry Delete Success | 0 |
| IPv6 Entry Delete Fail | 0 |
| IP Entry Override | 0 |
| IP Entry Add Req Skip | 0 |
| Data Glean Memory Req Recv | 0 |
| Data Glean Memory Req Fail | 0 |
| Data Glean Memory Reg Send | 0 |
| Data Glean Memory Ret Recv | 0 |
| Data Glean Memory Ret Send | 0 |
| Data Glean Entry Send | 0 |
| IPSG Subblock Allocate | 0 |
| IPSG Subblock Allocate Fail | 0 |
| IPSG Subblock Free | 0 |
| IPSG Subblock Free Fail | 0 |
| IPSG FIA Enable | 0 |
| IPSG FIA Enable Fail | 0 |
| IPSG FIA Disable | 0 |
| IPSG FIA Disable Fail | 0 |
| IPSG Feature Enable | 0 |
| IPSG Feature Enable Fail | 0 |
| IPSG Feature Disable | 0 |
| IPSG Feature Disable Fail | 0 |

----- show platform hardware chassis active qfp feature wireless ipsg cpp-client table ipv4 all -----

CPP Wireless IPSG Table Summary

Total number of address entries: 1

| IP Address | VLAN | uIDB |
|------------|------|-------|
| 177.1.0.7 | 177 | 95744 |

----- show platform hardware chassis active qfp feature wireless ipsg cpp-client table ipv6 all -----

CPP Wireless IPSG Table Summary

Total number of address entries: 0

----- show platform hardware chassis active qfp feature wireless ipsg datapath

```
statistics global -----
```

```
Wireless IPSG Global Statistics
```

```
-----
IPv6 Dataglean entry add      : 0
IPv6 Dataglean entry remove   : 0
IPv6 Dataglean allocation fail : 0
IPv6 Dataglean pool req send  : 0
IPv6 Dataglean pool req send fail : 0
IPv6 Dataglean pool req resp  : 0
IPv6 Dataglean pool ret send  : 0
IPv6 Dataglean pool ret send fail : 0
IPv6 Dataglean punt packet    : 0
IPv6 Dataglean drop packet    : 0
```

```
----- show platform hardware chassis active qfp feature wireless ipsg datapath
table ipv4 all -----
```

```
CPP Wireless IPSG IPv4 Table:
```

| IP Address | VLAN | uIDB | Interface |
|------------|------|-------|--------------------------|
| 177.1.0.7 | 177 | 95744 | WLCLIENT-IF-0x00a0000001 |

```
----- show platform hardware chassis active qfp feature wireless ipsg datapath
table ipv6 all -----
```

```
CPP Wireless IPSG IPv6 Table:
```

| IP Address | VLAN | uIDB | Interface |
|------------|------|------|-----------|
|------------|------|------|-----------|

```
----- show platform hardware chassis active qfp feature wireless halo statistics
-----
```

```
Wireless HALO Statistics
```

| | |
|-----------------|---|
| Rx Packet Count | 0 |
| Rx Packet Bytes | 0 |

```
----- show platform hardware chassis active qfp feature wireless fqdn-filter
summary -----
```

```
CPP Wireless FQDN Filter Info:
```

| ID | Type | DSA_hdl | Redirect_IPv4 | Virtual_IPv4 |
|----|------|---------|---------------|--------------|
|----|------|---------|---------------|--------------|

```
----- show platform hardware chassis active qfp feature wireless et-analytics
statistics -----
```

```
Wireless ETA cpp-client plumbing statistics
```

```
Number of ETA pending clients : 0
```

| Counter | Value |
|---------|-------|
|---------|-------|

```
-----  
Enable ETA on wireless client called      0  
Delete ETA on wireless client called      0  
ETA global cfg init cb TVI FIA enable error 0  
ETA global cfg init cb output SB read error 0  
ETA global cfg init cb output SB write error 0  
ETA global cfg init cb input SB read error 0  
ETA global cfg init cb input SB write error 0  
ETA global cfg init cb TVI FIA enable success 0  
ETA global cfg uninit cb ingress feat disable 0  
ETA global cfg uninit cb ingress cfg delete e 0  
ETA global cfg uninit cb egress feat disable 0  
ETA global cfg uninit cb egress cfg delete er 0  
ETA pending list insert entry called      0  
ETA pending list insert invalid arg error 0  
ETA pending list insert entry exists error 0  
ETA pending list insert no memory error    0  
ETA pending list insert entry failed      0  
ETA pending list insert entry success     0  
ETA pending list delete entry called      0  
ETA pending list delete invalid arg error 0  
ETA pending list delete entry missing     0  
ETA pending list delete entry remove error 0  
ETA pending list delete entry success     0
```

```
----- show platform hardware chassis active qfp feature wireless et-analytics  
eta-pending-client-tree -----
```

show tech-support wireless fabric

To display global fabric parameters, use the **show tech-support wireless fabric** command in privileged EXEC mode.

show tech-support wireless fabric

| | |
|---------------------------|--|
| 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 The output of the following commands are displayed as part of **show tech-support wireless fabric** command:

- show wireless fabric summary
- show wireless profile fabric summary
- show fabric wlan summary
- show fabric ap summary
- show wireless fabric client summary
- show wireless fabric media-stream client summary
- show wireless stats fabric memory
- show wireless stats fabric control-plane all

Example

The following is sample output from the **show tech-support wireless fabric** command

show tech-support wireless mobility

To print the data related to mobility, use the **show tech-support wireless mobility** command in privileged EXEC mode.

show tech-support wireless mobility

| | |
|---------------------------|--|
| Syntax Description | This command has no keywords or arguments. |
|---------------------------|--|

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

| | |
|----------------------|---------------------|
| Command Modes | Privileged EXEC (#) |
|----------------------|---------------------|

| Command History | Release | Modification |
|------------------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

Usage Guidelines The output of the following commands are displayed as part of **show tech-support wireless mobility** command:

- show platform hardware chassis active qfp feature wireless capwap cpp-client summary
- show platform hardware chassis active qfp feature wireless capwap datapath summary
- show platform hardware chassis active qfp feature wireless dtls cpp-client summary
- show platform hardware chassis active qfp feature wireless dtls datapath statistics
- show platform hardware chassis active qfp feature wireless dtls datapath summary
- show platform software capwap chassis active f0
- show platform software capwap chassis active r0
- show platform software dtls chassis active f0
- show platform software dtls chassis active r0
- show platform software ipc queue-based mobilityd chassis active R0 connection
- show platform software memory messaging mobilityd chassis active R0
- show platform software memory mobilityd chassis active R0 brief
- show wireless mobility ap-list
- show wireless mobility summary
- show wireless stats mobility
- show wireless stats mobility messages

In the presence of standby node, the output of the following mobility commands are also be displayed:

- show platform hardware chassis standby qfp feature wireless capwap cpp-client summary

- show platform hardware chassis standby qfp feature wireless capwap datapath summary
- show platform hardware chassis standby qfp feature wireless dtls cpp-client summary
- show platform hardware chassis standby qfp feature wireless dtls datapath statistics
- show platform hardware chassis standby qfp feature wireless dtls datapath summary
- show platform software capwap chassis standby f0
- show platform software capwap chassis standby r0
- show platform software dtls chassis standby f0
- show platform software dtls chassis standby r0
- show platform software ipc queue-based mobilityd chassis standby R0 connection
- show platform software memory messaging mobilityd chassis standby R0
- show platform software memory mobilityd chassis standby R0 brief
- show wireless stats mobility messages chassis standby r0

Example

The following is sample output from the **show tech-support wireless mobility** command

```
Device# show tech-support wireless mobility
----- show wireless stats mobility -----

Mobility event statistics:
  Joined as
    Local                : 0
    Foreign              : 0
    Export foreign       : 0
    Export anchor        : 0
  Delete
    Local                : 0
    Remote               : 0
  Role changes
    Local to anchor     : 0
    Anchor to local     : 0
  Roam stats
    L2 roam count       : 0
    L3 roam count       : 0
    Flex client roam count : 0
    Inter-WNCd roam count : 0
    Intra-WNCd roam count : 0
  Anchor Request
    Sent                : 0
    Grant received      : 0
    Deny received      : 0
  Received
    Grant sent          : 0
    Deny sent          : 0
  Handoff Status Received
    Success              : 0
    Group mismatch      : 0
```



```

Client unknown           : 0
Client blacklisted      : 0
SSID mismatch           : 0
Denied                   : 0
Handoff Status Sent
  Success                : 0
  Group mismatch         : 0
  Client unknown        : 0
  Client blacklisted    : 0
  SSID mismatch         : 0
  Denied                 : 0
Export Anchor
  Request Sent           : 0
  Response Received
    Ok                   : 0
    Deny - generic       : 0
    Client blacklisted   : 0
    Client limit reached : 0
    Profile mismatch     : 0
    Deny - unknown reason : 0
  Request Received      : 0
  Response Sent
    Ok                   : 0
    Deny - generic       : 0
    Client blacklisted   : 0
    Client limit reached : 0
    Profile mismatch     : 0
MM mobility event statistics:
  Event data allocs     : 0
  Event data frees     : 0
  FSM set allocs        : 0
  FSM set frees         : 0
  Timer allocs          : 0
  Timer frees           : 0
  Timer starts          : 0
  Timer stops           : 0
  Invalid events        : 0
  Internal errors       : 0

MMIF mobility event statistics:
  Event data allocs     : 0
  Event data frees     : 0
  Invalid events        : 0
  Unkown events         : 0
  Event schedule errors : 0
  Internal errors       : 0

```

----- show wireless stats mobility messages -----

```

MM datagram message statistics:
  Message Type      Built Tx   Rx   Processed Tx Error Rx Error Forwarded
  Retry Drops Allocs Frees
-----
  Mobile Announce   0    0   0    0         0         0         0
0    0    0    0
  Mobile Announce Nak 0    0   0    0         0         0         0
0    0    0    0

```

show tech-support wireless mobility

| | | | | | | | | |
|----------------------------|---|---|---|---|---|---|---|---|
| Static IP Mobile Annc | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 0 0 0 | | | | | | | | |
| Static IP Mobile Annc Rsp | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 0 0 0 | | | | | | | | |
| Handoff | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 0 0 0 | | | | | | | | |
| Handoff End | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 0 0 0 | | | | | | | | |
| Handoff End Ack | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 0 0 0 | | | | | | | | |
| Anchor Req | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 0 0 0 | | | | | | | | |
| Anchor Grant | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 0 0 0 | | | | | | | | |
| Anchor Xfer | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 0 0 0 | | | | | | | | |
| Anchor Xfer Ack | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 0 0 0 | | | | | | | | |
| Export Anchor Req | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 0 0 0 | | | | | | | | |
| Export Anchor Rsp | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 0 0 0 | | | | | | | | |
| AAA Handoff | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 0 0 0 | | | | | | | | |
| AAA Handoff Ack | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 0 0 0 | | | | | | | | |
| IPv4 Addr Update | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 0 0 0 | | | | | | | | |
| IPv4 Addr Update Ack | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 0 0 0 | | | | | | | | |
| IPv6 ND Packet | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 0 0 0 | | | | | | | | |
| IPv6 Addr Update | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 0 0 0 | | | | | | | | |
| IPv6 Addr Update Ack | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 0 0 0 | | | | | | | | |
| Client Add | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 0 0 0 | | | | | | | | |
| Client Delete | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 0 0 0 | | | | | | | | |
| Keepalive Ctrl Req | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 0 0 0 | | | | | | | | |
| Keepalive Ctrl Resp | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 0 0 0 | | | | | | | | |
| AP List Update | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 0 0 0 | | | | | | | | |
| Client Device Profile Info | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 0 0 0 | | | | | | | | |
| PMK Update | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 0 0 0 | | | | | | | | |
| PMK Delete | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 0 0 0 | | | | | | | | |
| PMK 11r Nonce Update | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 0 0 0 | | | | | | | | |
| Device cache Update | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 0 0 0 | | | | | | | | |
| HA SSO Announce | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 0 0 0 | | | | | | | | |
| HA SSO Announce Resp | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 0 0 0 | | | | | | | | |

MM IPC message statistics:

| Message Type | Built | Tx | Rx | Processed | Tx Error | Rx Error | Forwarded |
|--------------------|-------|----|----|-----------|----------|----------|-----------|
| Drops Allocs Frees | | | | | | | |

```

-----
Mobile Announce          0    0    0    0    0    0    0
0      0      0
Mobile Announce Nak     0    0    0    0    0    0    0
0      0      0
Static IP Mobile Annc   0    0    0    0    0    0    0
0      0      0
Static IP Mobile Annc Rsp 0    0    0    0    0    0    0
0      0      0
Handoff                  0    0    0    0    0    0    0
0      0      0
Handoff End             0    0    0    0    0    0    0
0      0      0
Handoff End Ack        0    0    0    0    0    0    0
0      0      0
Anchor Req              0    0    0    0    0    0    0
0      0      0
Anchor Grant            0    0    0    0    0    0    0
0      0      0
Anchor Xfer             0    0    0    0    0    0    0
0      0      0
Anchor Xfer Ack        0    0    0    0    0    0    0
0      0      0
Export Anchor Req      0    0    0    0    0    0    0
0      0      0
Export Anchor Rsp      0    0    0    0    0    0    0
0      0      0
AAA Handoff            0    0    0    0    0    0    0
0      0      0
AAA Handoff Ack        0    0    0    0    0    0    0
0      0      0
IPv4 Addr Update       0    0    0    0    0    0    0
0      0      0
IPv4 Addr Update Ack   0    0    0    0    0    0    0
0      0      0
IPv6 ND Packet         0    0    0    0    0    0    0
0      0      0
IPv6 Addr Update       0    0    0    0    0    0    0
0      0      0
IPv6 Addr Update Ack   0    0    0    0    0    0    0
0      0      0
Client Add              0    0    0    0    0    0    0
0      0      0
Client Delete          0    0    0    0    0    0    0
0      0      0
Keepalive Ctrl Req     0    0    0    0    0    0    0
0      0      0
Keepalive Ctrl Resp    0    0    0    0    0    0    0
0      0      0
AP List Update         0    0    0    0    0    0    0
0      0      0
Client Device Profile Info 0    0    0    0    0    0    0
0      0      0
PMK Update             0    0    0    0    0    0    0
0      0      0
PMK Delete             0    0    0    0    0    0    0
0      0      0
PMK 11r Nonce Update   0    0    0    0    0    0    0
0      0      0
Device cache Update    0    0    0    0    0    0    0
0      0      0
HA SSO Announce        0    0    0    0    0    0    0

```

show tech-support wireless mobility

```

0      0      0
  HA SSO Announce Resp      0      0      0      0      0      0      0
0      0      0
  
```

MMIF IPC message statistics:

| Message Type Frees | Built | Tx | Rx | Processed | Tx Error | Rx Error | Drops | Allocs |
|---------------------------------|-------|----|----|-----------|----------|----------|-------|--------|
| ----- | | | | | | | | |
| Mobile Announce 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Mobile Announce Nak 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Static IP Mobile Annc 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Static IP Mobile Annc Rsp 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Handoff 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Handoff End 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Handoff End Ack 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Anchor Req 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Anchor Grant 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Anchor Xfer 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Anchor Xfer Ack 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Export Anchor Req 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Export Anchor Rsp 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| AAA Handoff 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| AAA Handoff Ack 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| IPv4 Addr Update 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| IPv4 Addr Update Ack 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| IPv6 ND Packet 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| IPv6 Addr Update 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| IPv6 Addr Update Ack 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Client Add 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Client Delete 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Keepalive Ctrl Req 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Keepalive Ctrl Resp 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| AP List Update 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Client Device Profile Info 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| PMK Update 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

```

PMK Delete          0      0      0      0      0      0      0      0      0
0
PMK 11r Nonce Update 0      0      0      0      0      0      0      0      0
0
Device cache Update 0      0      0      0      0      0      0      0      0
0
HA SSO Announce     0      0      0      0      0      0      0      0      0
0
HA SSO Announce Resp 0      0      0      0      0      0      0      0      0
0
    
```

----- show wireless mobility summary -----

Mobility Summary

```

Wireless Management VLAN: 32
Wireless Management IP Address: 9.12.32.10
Mobility Control Message DSCP Value: 48
Mobility Keepalive Interval/Count: 10/3
Mobility Group Name: default
Mobility Multicast Ipv4 address: 0.0.0.0
Mobility Multicast Ipv6 address: ::
Mobility MAC Address: 001e.f6c1.f6ff
    
```

Controllers configured in the Mobility Domain:

| IP Multicast IPv6 | Public Ip | Group Name | Status | Multicast IPv4 PMTU | |
|-------------------|-----------|------------|--------|---------------------|----|
| 9.12.32.10 | N/A | default | N/A | 0.0.0.0 | :: |
| | | | | N/A | |

----- show wireless mobility ap-list -----

----- show platform software capwap chassis active r0 -----

----- show platform software capwap chassis active f0 -----

----- show platform software dtls chassis active r0 -----

----- show platform software dtls chassis active f0 -----

----- show platform hardware chassis active qfp feature wireless capwap
cpp-client summary -----

----- show platform hardware chassis active qfp feature wireless dtls cpp-client
summary -----

```
----- show platform hardware chassis active qfp feature wireless capwap datapath
summary -----
```

```
Vrf Src Port Dst IP          Dsp Port Input Uidb Output Uidb Instance Id
---  -----  -----  -----  -----  -----  -----  -----  -----
```

```
----- show platform hardware chassis active qfp feature wireless dtls datapath
statistics -----
```

CPP Wireless DTLS Feature Stats

| Description | Packet Count | Octet Count |
|--------------------------------------|--------------|-------------|
| DTLS Packets To Encrypt | 0 | 0 |
| DTLS Packets Encrypted | 0 | 0 |
| DTLS Packets To Decrypt | 0 | 0 |
| DTLS Packets Decrypted | 0 | 0 |
| Skip Encryption - Handshake | 0 | 0 |
| Skip Encryption - Not AppData | 0 | 0 |
| Skip Encryption - No Hash Entry | 0 | 0 |
| Skip Encryption - No Crypto Handle | 0 | 0 |
| Skip Encryption - No DTLS header | 0 | 0 |
| Skip Encryption - Requested by RP | 0 | 0 |
| Skip Decryption - Handshake | 0 | 0 |
| Skip Decryption - Not AppData | 0 | 0 |
| Skip Decryption - No Hash Entry | 0 | 0 |
| Skip Decryption - No Crypto Handle | 0 | 0 |
| Skip Decryption - No DTLS header | 0 | 0 |
| Skip Decryption - Multiple Records | 0 | 0 |
| Error - Encrypt Invalid Length | 0 | 0 |
| Error - Encrypt Header Restore | 0 | 0 |
| Error - DataEncrypt No Crypto Handle | 0 | 0 |
| Error - DataEncrypt Header Restore | 0 | 0 |
| Error - Decrypt Invalid Length | 0 | 0 |
| Error - Decrypt Header Restore | 0 | 0 |
| Error - DataDecrypt Zero Epoch | 0 | 0 |
| Error - DataDecrypt No Hash Entry | 0 | 0 |
| Error - DataDecrypt No Crypto Handle | 0 | 0 |
| Error - DataDecrypt Header Restore | 0 | 0 |

```
----- show platform hardware chassis active qfp feature wireless dtls datapath
summary -----
```

```
Src IP          Dst IP          Src Port Dst Port  Crypto HDL      Instance Id
-----  -----  -----  -----  -----  -----
```

```
----- show platform software ipc queue-based mobilityd chassis active R0
connection -----
```

```
Name: -mobilityd_to_wncd-b0
Number      : 0
Mode        : writer
Created on  : 03/22/18 05:35:06
Queue Size  : 524288 bytes, 0 bytes currently used
Enqueued    : 12 msgs, 432 bytes, 0 err, 0 back-pressures,
              360 bytes max queue utilization,
              0 times reached above 90%, 0 times reached above 75%
```

```
Name: -mobilityd_to_wncd-b1
  Number      : 1
  Mode        : writer
  Created on  : 03/22/18 05:35:06
  Queue Size  : 524288 bytes, 0 bytes currently used
  Enqueued    : 12 msgs, 432 bytes, 0 err, 0 back-pressures,
                360 bytes max queue utilization,
                0 times reached above 90%, 0 times reached above 75%

Name: -mobilityd_to_wncd-b2
  Number      : 2
  Mode        : writer
  Created on  : 03/22/18 05:35:06
  Queue Size  : 524288 bytes, 0 bytes currently used
  Enqueued    : 12 msgs, 432 bytes, 0 err, 0 back-pressures,
                360 bytes max queue utilization,
                0 times reached above 90%, 0 times reached above 75%

Name: -mobilityd_to_fman_rp-b0
  Number      : 3
  Mode        : writer
  Created on  : 03/22/18 05:35:06
  Queue Size  : 524288 bytes, 0 bytes currently used
  Enqueued    : 0 msgs, 0 bytes, 0 err, 0 back-pressures,
                0 bytes max queue utilization,
                0 times reached above 90%, 0 times reached above 75%

Name: -mobilityd_to_iosd_rp-b0
  Number      : 4
  Mode        : writer
  Created on  : 03/22/18 05:35:06
  Queue Size  : 524288 bytes, 0 bytes currently used
  Enqueued    : 204647 msgs, 15757819 bytes, 0 err, 0 back-pressures,
                81 bytes max queue utilization,
                0 times reached above 90%, 0 times reached above 75%

Name: -mobilityd_to_wncmgrd-b0
  Number      : 5
  Mode        : writer
  Created on  : 03/22/18 05:35:06
  Queue Size  : 524288 bytes, 0 bytes currently used
  Enqueued    : 12 msgs, 432 bytes, 0 err, 0 back-pressures,
                360 bytes max queue utilization,
                0 times reached above 90%, 0 times reached above 75%

Name: -odm_clnt2svr_data-mobilityd-000-1
  Number      : 6
  Mode        : writer
  Created on  : 03/22/18 05:35:06
  Queue Size  : 2097152 bytes, 0 bytes currently used
  Enqueued    : 33 msgs, 12535 bytes, 0 err, 0 back-pressures,
                3769 bytes max queue utilization,
                0 times reached above 90%, 0 times reached above 75%

Name: -odm_svr2clnt_data-mobilityd-000-1
  Number      : 7
  Mode        : reader
  Created on  : 03/22/18 05:35:06
  Queue Size  : 2097152 bytes, 0 bytes currently used
  Dequeued    : 0 msgs, 0 bytes, 0 err

Name: -fman_rp_to_mobilityd-b0
  Number      : 8
  Mode        : reader
```

show tech-support wireless mobility

```

Created on : 03/22/18 05:35:08
Queue Size : 524288 bytes, 0 bytes currently used
Dequeued  : 0 msgs, 0 bytes, 0 err

Name: -wncd_to_mobilityd-b0
Number   : 9
Mode     : reader
Created on : 03/22/18 05:35:13
Queue Size : 524288 bytes, 0 bytes currently used
Dequeued  : 39 msgs, 1404 bytes, 0 err

Name: -wncd_to_mobilityd-b1
Number   : 10
Mode     : reader
Created on : 03/22/18 05:35:13
Queue Size : 524288 bytes, 0 bytes currently used
Dequeued  : 39 msgs, 1404 bytes, 0 err

Name: -wncd_to_mobilityd-b2
Number   : 11
Mode     : reader
Created on : 03/22/18 05:35:14
Queue Size : 524288 bytes, 0 bytes currently used
Dequeued  : 39 msgs, 1404 bytes, 0 err

Name: -wncmgrd_to_mobilityd-b0
Number   : 12
Mode     : reader
Created on : 03/22/18 05:35:14
Queue Size : 524288 bytes, 0 bytes currently used
Dequeued  : 18 msgs, 648 bytes, 0 err

Name: -iosd_rp_to_mobilityd-b0
Number   : 13
Mode     : reader
Created on : 03/22/18 05:35:30
Queue Size : 1048576 bytes, 0 bytes currently used
Dequeued  : 204647 msgs, 18827524 bytes, 0 err

Name: -odm_clnt2svr_data-ifid-005-1
Number   : 14
Mode     : writer
Created on : 03/22/18 05:35:37
Queue Size : 2097152 bytes, 0 bytes currently used
Enqueued  : 0 msgs, 0 bytes, 0 err, 0 back-pressures,
           0 bytes max queue utilization,
           0 times reached above 90%, 0 times reached above 75%

Name: -odm_svr2clnt_data-ifid-005-1
Number   : 15
Mode     : reader
Created on : 03/22/18 05:35:37
Queue Size : 2097152 bytes, 0 bytes currently used
Dequeued  : 0 msgs, 0 bytes, 0 err

----- show platform software memory messaging mobilityd chassis active R0
-----

[tdl_toc] type toc_table_info/47da701cd9c36de7e888ca6d8dd80390/0 created:3 destroyed:3
diff:0
[tdl_sr] type repl_table_name/29184a6d15c1ball1acb2d0bd22eb6e36/0 created:33 destroyed:33
diff:0

```



```
[tdl_sr] type repl_database_name/e9118a691a20b4b8f1118bc37a894603/0 created:33 destroyed:33
diff:0
[tdl_sr] type repl_pkey_tdl/83de2d20ec3ca19b8ae9a89147480a25/1 created:33 destroyed:33
diff:0
[tdl_sr] type repl_blob_tdl/016a67083ea407334130436c855ae237/0 created:33 destroyed:33
diff:0
[tdl_sr] type repl_luid/b9c9d9f4876af528cb82273df98479d6/0 created:33 destroyed:33 diff:0
[tdl_sr] type repl_objinfo/6c8800fedf8d71512f9b6c9754db3a70/0 created:33 destroyed:33 diff:0
[tdl_sr] message repl_trec_update/15fe2a39409473179c9e7111851b2196/0 created:33 destroyed:33
diff:0
[pki_ssl] type buff/941d8a519d6f23d27067617119f1bb38/0 created:613944 destroyed:613944
diff:0
[pki_ssl] type get_certid_params/0d7bcce690f74649c2e33bbf341e2229/0 created:204648
destroyed:204648 diff:0
[pki_ssl] type get_certid_callback_params/708b7fb964ace7971d90a452c830488c/0 created:204648
destroyed:204648 diff:0
[pki_ssl] message get_certid/ee3bfe6b93901440346417a4ad67fa63/0 created:204648
destroyed:204648 diff:0
[pki_ssl] message get_certid_callback/372218059d7a753ba73f7b06f18532e9/0 created:204648
destroyed:204648 diff:0
[svc_defs] type svc_loc/929237802cf26e862f8e8716169e31ef/0 created:40952 destroyed:40951
diff:1
[ui_shr] type ui_client/bec7457db0c33cae9eeebbf80073b771/0 created:3 destroyed:2 diff:1
[ui] type ui_info/4b8b42a883fabbb98ec8b919f60e4ad6/0 created:40949 destroyed:40949 diff:0
[ui] type ui_req/69f1e2a5943e050f0aa12df8639ba442/0 created:3 destroyed:2 diff:1
[ui] type event_statistics/7f346ee47165c035a72e139b84afb2a0/0 created:40948 destroyed:40948
diff:0
[ui] type hostinfo_data/54d5a8b0cd4d29d575b2fc0d91695b5e/0 created:3 destroyed:3 diff:0
[ui] message ui_info_msg/bec533dd713e0222cb8fe5df868031f0/0 created:1 destroyed:1 diff:0
[ui] message ui_req_msg/ac9905cc4488c976847affab56d8b50c/0 created:3 destroyed:2 diff:1
[ui] message process_event_statistics/65d07aa3a04ad950cddd46444df6bc02/0 created:40948
destroyed:40948 diff:0
[ui] message hostinfo_notify/2e9d975712b85b41bc489a6adbc4a46c/0 created:3 destroyed:3 diff:0
[uipeer_comm_ui] type mqipc_enqueue_stats/8f41e408c97a799a5e431d2279acd8de/0 created:8
destroyed:8 diff:0
[uipeer_comm_ui] type mqipc_dequeue_stats/aafe5d0a37ba9652d68550efa26eb0b6/0 created:8
destroyed:8 diff:0
[uipeer_comm_ui] type mqipc_connection_properties/35bd274fd85f7359066f898f25c853ee/0
created:16 destroyed:16 diff:0
[uipeer_comm_ui] message mqipc_connection/a1b22c74b279335b895531ce708c804b/0 created:16
destroyed:16 diff:0
[mem_stats_ui] type tdl_variant_stat/bd85e4b89fb10501e68c1a3cedb9f321/0 created:1 destroyed:0
diff:1
[mem_stats_ui] message tdl_mem_stats/60ffd9d51213767d041b543869df15d2/0 created:1 destroyed:0
diff:1
[cdlcore] type cdl_params/a3e74327d37abf27f799f2b5155f4923/0 created:2 destroyed:1 diff:1
[cdlcore] message cdl_message/35205e535c7ab2cdcb3c265ac788f973/0 created:2 destroyed:1
diff:1
[odm_defs] type odm_context/73aeeeb77a1ccb6e44f690745cdafe0d/1 created:23 destroyed:23
diff:0
[odm_defs] type odm_register_info/48a7d590e9df0cc9d150801315c50307/1 created:4 destroyed:4
diff:0
[odm_defs] type odm_table_register_info/4f355a34615affd49af9f90b679d8ce5/1 created:17
destroyed:17 diff:0
[odm_defs] type odm_register_result/53ba304bc0a71a7d2a044518c21f662a/0 created:2 destroyed:2
diff:0
[odm_defs] message odm_register/2c98272b43d973fa08bbf5acdf3106b0/0 created:2 destroyed:2
diff:0
[odm_defs] message odm_table_register/46694ec1005c3b084337748eeb3768cd/0 created:17
destroyed:17 diff:0
[odm_defs] message odm_register_done/1f6c8f81fcbb8a3052428bab7588e8b5/0 created:2 destroyed:2
diff:0
[odm_defs] message odm_register_ack/03b8040ed4f7b03517b410c32568ecaa/0 created:2 destroyed:2
diff:0
```

```
----- show platform software memory mobilityd chassis active R0 brief
-----
```

| module | allocated | requested | allocs | frees |
|-------------------|-----------|-----------|--------|-------|
| Summary | 620441 | 617113 | 233 | 25 |
| unknown | 198515 | 198435 | 5 | 0 |
| chunk | 139689 | 139209 | 30 | 0 |
| eventutil | 118939 | 118299 | 48 | 8 |
| process | 67642 | 67594 | 3 | 0 |
| odm-db-ctx | 29950 | 28430 | 100 | 5 |
| uippeer | 22672 | 22592 | 11 | 6 |
| odm-ipc-ctx | 20272 | 19984 | 18 | 0 |
| unknown | 18024 | 18008 | 1 | 0 |
| odm-client-ctx | 1872 | 1824 | 3 | 0 |
| cdllib | 1688 | 1672 | 3 | 2 |
| trccfg | 512 | 496 | 5 | 4 |
| bidb | 472 | 456 | 1 | 0 |
| unknown | 96 | 48 | 3 | 0 |
| bcrdu_avl | 72 | 56 | 1 | 0 |
| orchestrator_main | 26 | 10 | 1 | 0 |

show tech-support wireless radio

To print the data related to the radio, use the **show tech-support wireless radio** command in privileged EXEC mode.

show tech-support wireless radio

| | |
|---------------------------|--|
| 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 The output of the following commands are displayed as part of **show tech-support wireless radio** command:

- show ap auto-rf dot11 24ghz
- show ap auto-rf dot11 5ghz
- show ap config dot11 dual-band summary
- show ap config general
- show ap dot11 24ghz channel
- show ap dot11 24ghz coverage
- show ap dot11 24ghz group
- show ap dot11 24ghz high-density
- show ap dot11 24ghz load-info
- show ap dot11 24ghz monitor
- show ap dot11 24ghz network
- show ap dot11 24ghz summary
- show ap dot11 24ghz txpower
- show ap dot11 5ghz channel
- show ap dot11 5ghz coverage
- show ap dot11 5ghz group
- show ap dot11 5ghz high-density
- show ap dot11 5ghz load-info

- show ap dot11 5ghz monitor
- show ap dot11 5ghz network
- show ap dot11 5ghz summary
- show ap dot11 5ghz txpower
- show ap fra
- show ap rf-profile name Rfl detail
- show ap rf-profile summary
- show ap summary
- show wireless band-select

Example

The following is sample output from the **show tech-support wireless radio** command

```
Device# show tech-support wireless radio
----- show ap summary -----

Number of APs: 0

----- show ap dot11 24ghz summary -----

----- show ap dot11 5ghz summary -----

----- show ap config dot11 dual-band summary -----

----- show ap dot11 24ghz channel -----

Leader Automatic Channel Assignment
Channel Assignment Mode           : AUTO
Channel Update Interval           : 600 seconds
Anchor time (Hour of the day)     : 0
Channel Update Contribution
  Noise                           : Enable
  Interference                     : Enable
  Load                            : Disable
  Device Aware                    : Disable
CleanAir Event-driven RRM option  : Disabled
Channel Assignment Leader         : ewlc-doc (9.12.32.10)
Last Run                          : 550 seconds ago

DCA Sensitivity Level              : MEDIUM : 10 dB
DCA Minimum Energy Limit          : -95 dBm
Channel Energy Levels
```

```

Minimum                               : unknown
Average                               : unknown
Maximum                               : -128 dBm
Channel Dwell Times
Minimum                               : unknown
Average                               : unknown
Maximum                               : unknown
802.11b 2.4 GHz Auto-RF Channel List
Allowed Channel List                   : 1,6,11
Unused Channel List                   : 2,3,4,5,7,8,9,10

```

----- show ap dot11 5ghz channel -----

```

Leader Automatic Channel Assignment
Channel Assignment Mode                 : AUTO
Channel Update Interval                : 600 seconds
Anchor time (Hour of the day)          : 0
Channel Update Contribution
  Noise                               : Enable
  Interference                         : Enable
  Load                                : Disable
  Device Aware                         : Disable
CleanAir Event-driven RRM option       : Disabled
Channel Assignment Leader               : ewlc-doc (9.12.32.10)
Last Run                               : 552 seconds ago

DCA Sensitivity Level                  : MEDIUM : 15 dB
DCA 802.11n/ac Channel Width           : 20 MHz
DCA Minimum Energy Limit               : -95 dBm
Channel Energy Levels
  Minimum                             : unknown
  Average                             : unknown
  Maximum                             : -128 dBm
Channel Dwell Times
  Minimum                             : unknown
  Average                             : unknown
  Maximum                             : unknown
802.11a 5 GHz Auto-RF Channel List
Allowed Channel List                   :
36,40,44,48,52,56,60,64,100,104,108,112,116,120,124,128,132,136,140,144,149,153,157,161
Unused Channel List                   : 165

```

----- show ap dot11 24ghz coverage -----

```

Coverage Hole Detection
802.11b Coverage Hole Detection Mode   : Enabled
802.11b Coverage Voice Packet Count   : 100 packet(s)
802.11b Coverage Voice Packet Percentage : 50%
802.11b Coverage Voice RSSI Threshold : -80 dBm
802.11b Coverage Data Packet Count    : 50 packet(s)
802.11b Coverage Data Packet Percentage : 50%
802.11b Coverage Data RSSI Threshold  : -80 dBm
802.11b Global coverage exception level : 25 %
802.11b Global client minimum exception level : 3 clients

```

----- show ap dot11 5ghz coverage -----

```

Coverage Hole Detection

```

```

802.11a Coverage Hole Detection Mode      : Enabled
802.11a Coverage Voice Packet Count     : 100 packet(s)
802.11a Coverage Voice Packet Percentage : 50 %
802.11a Coverage Voice RSSI Threshold   : -80dBm
802.11a Coverage Data Packet Count      : 50 packet(s)
802.11a Coverage Data Packet Percentage : 50 %
802.11a Coverage Data RSSI Threshold    : -80dBm
802.11a Global coverage exception level  : 25 %
802.11a Global client minimum exception level : 3 clients

```

```
----- show ap dot11 24ghz group -----
```

Radio RF Grouping

```

802.11b Group Mode           : AUTO
802.11b Group Update Interval : 600 seconds
802.11b Group Leader         : ewlc-doc (9.12.32.10)
802.11b Last Run             : 553 seconds ago

```

RF Group Members

```

Controller name           Controller IP
-----
ewlc-doc                   9.12.32.10

```

```
----- show ap dot11 5ghz group -----
```

Radio RF Grouping

```

802.11a Group Mode           : AUTO
802.11a Group Update Interval : 600 seconds
802.11a Group Leader         : ewlc-doc (9.12.32.10)
802.11a Last Run             : 553 seconds ago

```

RF Group Members

```

Controller name           Controller IP
-----
ewlc-doc                   9.12.32.10

```

```
----- show ap dot11 24ghz high-density -----
```

```
----- show ap dot11 5ghz high-density -----
```

```
----- show ap dot11 5ghz load-info -----
```

```
----- show ap dot11 24ghz load-info -----
```

----- show ap dot11 24ghz profile -----

```

Default 802.11b AP performance profiles
 802.11b Global Interference threshold      : 10 %
 802.11b Global noise threshold            : -70 dBm
 802.11b Global RF utilization threshold    : 80 %
 802.11b Global throughput threshold        : 1000000 bps
 802.11b Global clients threshold          : 12 clients
    
```

----- show ap dot11 5ghz profile -----

```

Default 802.11a AP performance profiles

 802.11a Global Interference threshold      : 10 %
 802.11a Global noise threshold            : -70 dBm
 802.11a Global RF utilization threshold    : 80 %
 802.11a Global throughput threshold        : 1000000 bps
 802.11a Global clients threshold          : 12 clients
    
```

----- show ap dot11 24ghz monitor -----

```

Default 802.11b AP monitoring
 802.11b Monitor Mode                      : Enabled
 802.11b Monitor Channels                  : Country channels
 802.11b RRM Neighbor Discover Type        : Transparent
 802.11b AP Coverage Interval              : 180 seconds
 802.11b AP Load Interval                  : 60 seconds
 802.11b AP Noise Interval                 : 180 seconds
 802.11b AP Signal Strength Interval       : 60 seconds
 802.11b NDP RSSI Normalization            : Enabled
    
```

----- show ap dot11 5ghz monitor -----

```

Default 802.11a AP monitoring
 802.11a Monitor Mode                      : Enabled
 802.11a Monitor Channels                  : Country channels
 802.11a RRM Neighbor Discover Type        : Transparent
 802.11a AP Coverage Interval              : 180 seconds
 802.11a AP Load Interval                  : 60 seconds
 802.11a AP Noise Interval                 : 180 seconds
 802.11a AP Signal Strength Interval       : 60 seconds
 802.11a NDP RSSI Normalization            : Enabled
    
```

----- show ap dot11 24ghz network -----

```

802.11b Network                          : Enabled
11gSupport                                : Enabled
11nSupport                                : Enabled
802.11b/g Operational Rates
 802.11b 1M                               : Mandatory
    
```

```

802.11b 2M : Mandatory
802.11b 5.5M : Mandatory
802.11b 11M : Mandatory
802.11g 6M : Supported
802.11g 9M : Supported
802.11g 12M : Supported
802.11g 18M : Supported
802.11g 24M : Supported
802.11g 36M : Supported
802.11g 48M : Supported
802.11g 54M : Supported
802.11n MCS Settings:
MCS 0 : Supported
MCS 1 : Supported
MCS 2 : Supported
MCS 3 : Supported
MCS 4 : Supported
MCS 5 : Supported
MCS 6 : Supported
MCS 7 : Supported
MCS 8 : Supported
MCS 9 : Supported
MCS 10 : Supported
MCS 11 : Supported
MCS 12 : Supported
MCS 13 : Supported
MCS 14 : Supported
MCS 15 : Supported
MCS 16 : Supported
MCS 17 : Supported
MCS 18 : Supported
MCS 19 : Supported
MCS 20 : Supported
MCS 21 : Supported
MCS 22 : Supported
MCS 23 : Supported
MCS 24 : Supported
MCS 25 : Supported
MCS 26 : Supported
MCS 27 : Supported
MCS 28 : Supported
MCS 29 : Supported
MCS 30 : Supported
MCS 31 : Supported
802.11n Status:
A-MPDU Tx:
Priority 0 : Enabled
Priority 1 : Disabled
Priority 2 : Disabled
Priority 3 : Disabled
Priority 4 : Enabled
Priority 5 : Enabled
Priority 6 : Disabled
Priority 7 : Disabled
Aggregation scheduler : Enabled
Realtime timeout : 10
A-MSDU Tx:
Priority 0 : Enable
Priority 1 : Enable
Priority 2 : Enable
Priority 3 : Enable
Priority 4 : Enable
Priority 5 : Enable
Priority 6 : Disable

```



```

Priority 7 : Disable
Guard Interval : Any
Rifs Rx : Enabled
Beacon Interval : 100
CF Pollable mandatory : Disabled
CF Poll Request Mandatory : Disabled
CFP Period : 4
CFP Maximum Duration : 60
Default Channel : 1
Default Tx Power Level : 1
DTPC Status : Enabled
Call Admission Limit :
G711 CU Quantum :
ED Threshold : -50
Fragmentation Threshold : 2346
RSSI Low Check : Disabled
RSSI Threshold : -127 dbm
PBCC Mandatory : unknown
Pico-Cell-V2 Status : unknown
RTS Threshold : 2347
Short Preamble Mandatory : Enabled
Short Retry Limit : 7
Legacy Tx Beamforming setting : Disabled
Traffic Stream Metrics Status : Disabled
Expedited BW Request Status : Disabled
EDCA profile type check : default-wmm
Call Admission Control (CAC) configuration
Voice AC
Voice AC - Admission control (ACM) : Disabled
Voice Stream-Size : 84000
Voice Max-Streams : 2
Voice Max RF Bandwidth : 75
Voice Reserved Roaming Bandwidth : 6
Voice Load-Based CAC mode : Enabled
Voice tspec inactivity timeout : Enabled
CAC SIP-Voice configuration
SIP based CAC : Disabled
SIP call bandwidth : 64
SIP call bandwidth sample-size : 20
Maximum Number of Clients per AP Radio : 200

```

```
----- show ap dot11 5ghz network -----
```

```

802.11a Network : Enabled
11nSupport : Enabled
802.11a Low Band : Enabled
802.11a Mid Band : Enabled
802.11a High Band : Enabled
802.11a Operational Rates
802.11a 6M : Mandatory
802.11a 9M : Supported
802.11a 12M : Mandatory
802.11a 18M : Supported
802.11a 24M : Mandatory
802.11a 36M : Supported
802.11a 48M : Supported
802.11a 54M : Supported
802.11n MCS Settings:
MCS 0 : Supported
MCS 1 : Supported
MCS 2 : Supported

```

```

MCS 3 : Supported
MCS 4 : Supported
MCS 5 : Supported
MCS 6 : Supported
MCS 7 : Supported
MCS 8 : Supported
MCS 9 : Supported
MCS 10 : Supported
MCS 11 : Supported
MCS 12 : Supported
MCS 13 : Supported
MCS 14 : Supported
MCS 15 : Supported
MCS 16 : Supported
MCS 17 : Supported
MCS 18 : Supported
MCS 19 : Supported
MCS 20 : Supported
MCS 21 : Supported
MCS 22 : Supported
MCS 23 : Supported
MCS 24 : Supported
MCS 25 : Supported
MCS 26 : Supported
MCS 27 : Supported
MCS 28 : Supported
MCS 29 : Supported
MCS 30 : Supported
MCS 31 : Supported
802.11n Status:
A-MPDU Tx:
  Priority 0 : Enabled
  Priority 1 : Disabled
  Priority 2 : Disabled
  Priority 3 : Disabled
  Priority 4 : Enabled
  Priority 5 : Enabled
  Priority 6 : Disabled
  Priority 7 : Disabled
  Aggregation scheduler : Enabled
  Realtime timeout : 10
A-MSDU Tx:
  Priority 0 : Enable
  Priority 1 : Enable
  Priority 2 : Enable
  Priority 3 : Enable
  Priority 4 : Enable
  Priority 5 : Enable
  Priority 6 : Disable
  Priority 7 : Disable
  Guard Interval : Any
Rifs Rx : Enabled
802.11ac : Enabled
  Frame burst : Automatic
802.11ac MCS Settings:
Beacon Interval : 100
CF Pollable mandatory : Disabled
CF Poll Request Mandatory : Disabled
CFP Period : 4
CFP Maximum Duration : 60
Default Channel : 36
Default Tx Power Level : 1
DTPC Status : Enabled
Fragmentation Threshold : 2346

```

```

RSSI Low Check                : Disabled
RSSI Threshold                 : -127 dbm
Pico-Cell-V2 Status           : unknown
TI Threshold                   :
Legacy Tx Beamforming setting  : Disabled
Traffic Stream Metrics Status  : Disabled
Expedited BW Request Status   : Disabled
EDCA profile type check       : default-wmm
Call Admission Control (CAC) configuration
Voice AC
  Voice AC - Admission control (ACM) : Disabled
  Voice Stream-Size                : 84000
  Voice Max-Streams                 : 2
  Voice Max RF Bandwidth            : 75
  Voice Reserved Roaming Bandwidth : 6
  Voice Load-Based CAC mode        : Enabled
  Voice tspec inactivity timeout   : Enabled
CAC SIP-Voice configuration
  SIP based CAC                    : Disabled
  SIP call bandwidth                : 64
  SIP call bandwidth sample-size   : 20
Maximum Number of Clients per AP Radio : 200

```

----- show ap dot11 24ghz txpower -----

Automatic Transmit Power Assignment

```

Transmit Power Assignment Mode : AUTO
Transmit Power Update Interval : 600 seconds
Transmit Power Threshold       : -70 dBm
Transmit Power Neighbor Count  : 3 APs
Min Transmit Power              : -10 dBm
Max Transmit Power              : 30 dBm
Update Contribution
  Noise                          : Enable
  Interference                    : Enable
  Load                           : Disable
  Device Aware                    : Disable
Transmit Power Assignment Leader : ewlc-doc (9.12.32.10)
Last Run                        : 558 seconds ago

```

----- show ap dot11 5ghz txpower -----

Automatic Transmit Power Assignment

```

Transmit Power Assignment Mode : AUTO
Transmit Power Update Interval : 600 seconds
Transmit Power Threshold       : -70 dBm
Transmit Power Neighbor Count  : 3 APs
Min Transmit Power              : -10 dBm
Max Transmit Power              : 30 dBm
Update Contribution
  Noise                          : Enable
  Interference                    : Enable
  Load                           : Disable
  Device Aware                    : Disable
Transmit Power Assignment Leader : ewlc-doc (9.12.32.10)
Last Run                        : 558 seconds ago

```

```
----- show ap auto-rf dot11 5ghz -----
```

```
----- show ap auto-rf dot11 24ghz -----
```

```
----- show ap config general -----
```

```
----- show ap dot11 5ghz optimized-roaming -----
```

```
802.11a OptimizedRoaming
```

```
Mode : Disabled
Reporting Interval : 90 seconds
Rate Threshold : Disabled
Hysteresis : 6 db
```

```
----- show ap rf-profile summary -----
```

```
Number of RF-profiles: 6
```

| RF Profile Name | Band | Description | State |
|--------------------------------|---------|--------------------------------------|-------|
| Low_Client_Density_rf_5gh | 5 GHz | pre configured Low Client Density rf | Up |
| High_Client_Density_rf_5gh | 5 GHz | pre configured High Client Density r | Up |
| Low_Client_Density_rf_24gh | 2.4 GHz | pre configured Low Client Density rf | Up |
| High_Client_Density_rf_24gh | 2.4 GHz | pre configured High Client Density r | Up |
| Typical_Client_Density_rf_5gh | 5 GHz | pre configured Typical Density rfpro | Up |
| Typical_Client_Density_rf_24gh | 2.4 GHz | pre configured Typical Client Densit | Up |

```
----- show ap fra -----
```

```
FRA State : Disabled
FRA Sensitivity : medium (95%)
FRA Interval : 1 Hour(s)
  Last Run : 2299 seconds ago
  Last Run time : 0 seconds
```

| AP Name | MAC Address | Slot ID | Current-Band | COF % | Suggested Mode |
|---------|-------------|---------|--------------|-------|----------------|
|---------|-------------|---------|--------------|-------|----------------|

```
COF : Coverage Overlap Factor
```

```
----- show wireless band-select -----
```

```
Band Select Probe Response : per WLAN enabling
Cycle Count : 2
Cycle Threshold (millisec) : 200
Age Out Suppression (sec) : 20
Age Out Dual Band (sec) : 60
Client RSSI (dBm) : -80
Client Mid RSSI (dBm) : -80
```

```
----- show wireless country configure -----
```

```
Configured Country..... US - United States
Configured Country Codes
    US - United States          802.11a Indoor/ 802.11b Indoor/ 802.11g Indoor
```

```
----- show wireless tag rf summary -----
```

```
Number of RF Tags: 1
```

```
RF tag name          Description
-----
default-rf-tag      default RF tag
```

```
----- show ap tag summary -----
```

```
Number of APs: 0
```

```
----- show ap status -----
```

```
----- show ap uptime -----
```

```
Number of APs: 0
```

show tunnel eogre global-configuration

To display the Ethernet over GRE (EoGRE) global configuration, use the **show tunnel eogre global-configuration** command.

show tunnel eogre global-configuration

| | | |
|---------------------------|--|------------------------------|
| Syntax Description | This command has no keywords or arguments. | |
| Command Default | None | |
| Command Modes | Privileged EXEC (#) | |
| Command History | Release | Modification |
| | Cisco IOS XE Gibraltar 16.11.1 | This command was introduced. |

Example

This example shows how to display the EoGRE global configuration:

```
Device# show tunnel eogre global-configuration

Heartbeat interval      : 60
Max Heartbeat skip count : 3
Source Interface        : (none)
```

show tunnel eogre domain detailed

To display the detailed information of the Ethernet over GRE (EoGRE) tunnel domain, use the **show tunnel eogre domain detailed** command.

show tunnel eogre domain detailed *domain-name*

| | | |
|---------------------------|---------------------------------------|------------------------------|
| Syntax Description | <i>domain-name</i> EoGRE domain name. | |
| Command Default | None | |
| Command Modes | Privileged EXEC (#) | |
| Command History | Release | Modification |
| | Cisco IOS XE Gibraltar 16.11.1 | This command was introduced. |

Example

This example shows how to display the detailed information of the EoGRE tunnel domain:

```
Device# show tunnel eogre domain detailed eogre_domain

Domain Name      : eogre_domain
Primary GW       : Tunnel1
Secondary GW     : Tunnel2
Active GW        : Tunnel1
Redundancy       : Non-Revertive
```

show tunnel eogre domain summary

To display the summary information of the Ethernet over GRE (EoGRE) tunnel domain, use the **show tunnel eogre domain summary** command.

show tunnel eogre domain summary

| | |
|---------------------------|--|
| Syntax Description | This command has no keywords or arguments. |
|---------------------------|--|

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

| | |
|----------------------|---------------------|
| Command Modes | Privileged EXEC (#) |
|----------------------|---------------------|

| | | |
|------------------------|--------------------------------|------------------------------|
| Command History | Release | Modification |
| | Cisco IOS XE Gibraltar 16.11.1 | This command was introduced. |

Example

This example shows how to display the summary information of the EoGRE tunnel domain:

```
Device# show tunnel eogre domain summary
```

| Domain Name | Primary GW | Secondary GW | Active GW | Redundancy |
|--------------|------------|--------------|-----------|---------------|
| domain1 | Tunnel1 | Tunnel2 | Tunnel1 | Non-Revertive |
| eogre_domain | Tunnel1 | Tunnel2 | Tunnel1 | Non-Revertive |

show tunnel eogre gateway summary

To display the summary information of the Ethernet over GRE (EoGRE) tunnel gateway, use the **show tunnel eogre gateway summary** command.

show tunnel eogre gateway summary

| Syntax Description | This command has no keywords or arguments. | | | | |
|--------------------------------|--|---------|--------------|--------------------------------|------------------------------|
| Command Default | None | | | | |
| Command Modes | Privileged EXEC (#) | | | | |
| Command History | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.11.1</td> <td>This command was introduced.</td> </tr> </tbody> </table> | Release | Modification | Cisco IOS XE Gibraltar 16.11.1 | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE Gibraltar 16.11.1 | This command was introduced. | | | | |

Example

This example shows how to display the summary information of the EoGRE tunnel gateway:

```
Device# show tunnel eogre gateway summary
```

| Name | Type | Address | AdminState | State | Clients |
|-----------|------|-----------------|------------|-------|---------|
| Tunnel1 | IPv4 | 9.51.1.11 | Up | Up | 0 |
| Tunnel2 | IPv4 | 9.51.1.12 | Up | Down | 0 |
| Tunnel10 | IPv6 | fd09:9:8:21::90 | Down | Down | 0 |
| Tunnel11 | IPv4 | 9.51.1.11 | Up | Up | 0 |
| Tunnel12 | IPv6 | fd09:9:8:21::90 | Up | Down | 0 |
| Tunnel100 | IPv4 | 9.51.1.100 | Up | Down | 0 |

show tunnel eogre gateway detailed

To display the detailed information of the Ethernet over GRE (EoGRE) tunnel domain, use the **show tunnel eogre gateway detailed** command.

show tunnel eogre gateway detailed *gateway-name*

| Syntax Description | <i>gateway-name</i> EoGRE gateway name. | | | | |
|--------------------------------|--|---------|--------------|--------------------------------|------------------------------|
| Command Default | None | | | | |
| Command Modes | Privileged EXEC (#) | | | | |
| Command History | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.11.1</td> <td>This command was introduced.</td> </tr> </tbody> </table> | Release | Modification | Cisco IOS XE Gibraltar 16.11.1 | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE Gibraltar 16.11.1 | This command was introduced. | | | | |

Example

This example shows how to display the detailed information of the EoGRE tunnel gateway:

```
Device# show tunnel eogre domain detailed Tunnell
```

```
Gateway : Tunnell
Mode    : IPv4
IP      : 9.51.1.11
Source  : Vlan51 / 9.51.1.1
State   : Up
SLA ID  : 56
MTU     : 1480
Up Time: 4 minutes 45 seconds

Clients
  Total Number of Wireless Clients      : 0
Traffic
  Total Number of Received Packets      : 0
  Total Number of Received Bytes        : 0
  Total Number of Transmitted Packets   : 0
  Total Number of Transmitted Bytes     : 0
Keepalives
  Total Number of Lost Keepalives       : 0
  Total Number of Received Keepalives   : 5
  Total Number of Transmitted Keepalives: 5
Windows
  Transmitted Keepalives in last window : 2
  Received Keepalives in last window    : 2
```

show tunnel eogre manager stats global

To display the global tunnel manager statistics, use the **show tunnel eogre manager stats global** command.

show tunnel eogre manager stats global

| | | |
|---------------------------|--|------------------------------|
| Syntax Description | This command has no keywords or arguments. | |
| Command Default | None | |
| Command Modes | Privileged EXEC (#) | |
| Command History | Release | Modification |
| | Cisco IOS XE Gibraltar 16.11.1 | This command was introduced. |

Example

This example shows how to display the global tunnel manager statistics:

```
Device# show tunnel eogre manager stats global

Tunnel Global Statistics
Last Updated                : 02/18/2019 23:50:35
EoGRE Objects
  Gateways                   : 6
  Domains                     : 2

EoGRE Flex Objects
  AP Gateways                 : 2
  AP Domains                   : 1
  AP Gateways HA inconsistencies : 0
  AP Domains HA inconsistencies : 0

Config events
  IOS Tunnel updates          : 806
  IOS Domain updates          : 88
  Global updates               : 48
  Tunnel Profile updates      : 120
  Tunnel Rule updates         : 16
  AAA proxy key updates       : 0

AP events
  Flex AP Join                 : 1
  Flex AP Leave                 : 0
  Local AP Join                 : 0
  Local AP leave                : 0
  Tunnel status (rx)           : 4
  Domain status (rx)           : 1
  IAPP stats msg (rx)          : 3
  Client count (rx)            : 6
  VAP Payload msg (tx)         : 4
  Domain config (tx)           : 1
  Global config (tx)           : 1
  Client delete (tx)           : 1
```

show tunnel eogre manager stats global

```

Client delete per domain (tx) : 3
DHCP option 82 (tx) : 4

Client events
Add-mobile : 2
Run-State : 3
Delete : 1
Cleanup : 0
Join : 2
Plumb : 0
Join Errors : 0
HandOff : 0
MsPayload : 2
FT Recover : 0
Zombie GW counter increase : 0
Zombie GW counter decrease : 0
Tunnel Profile reset : 88
Client deauth : 0
HA reconciliation : 0

Client Join Events
Generic Error : 0
MSPayload Fail : 0
Invalid VLAN : 0
Invalid Domain : 0
No GWs in Domain : 0
Domain Shut : 0
Invalid GWs : 0
GWs Down : 0
Rule Match Error : 0
AAA-override : 0
Flex No Active GW : 0
Open Auth join attempt : 2
Dotlx join attempt : 2
Mobility join attempt : 0
Tunnel Profile not valid : 2
Tunnel Profile valid : 2
No rule match : 0
Rule match : 2
AAA proxy : 0
AAA proxy accounting : 0
AAA eogre attributes : 0
Has aaa override : 0
Error in handoff payload : 0
Handoff AAA override : 0
Handoff no AAA override : 0
Handoff payload received : 0
Handoff payload sent : 0

SNMP Traps
Client : 0
Tunnel : 2
Domain : 0

IPC
IOSd TX messages : 0

Zombie Client
Entries : 0

```

show tunnel eogre manager stats instance

To display the tunnel manager statistics for a specific WNCd instance, use the **show tunnel eogre manager stats instance** command.

show tunnel eogre manager stats instance *instance-number*

| Syntax Description | <i>instance-number</i> WNCd instance number. | | | | |
|--------------------------------|--|---------|--------------|--------------------------------|------------------------------|
| Command Default | None | | | | |
| Command Modes | Privileged EXEC (#) | | | | |
| Command History | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.11.1</td> <td>This command was introduced.</td> </tr> </tbody> </table> | Release | Modification | Cisco IOS XE Gibraltar 16.11.1 | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE Gibraltar 16.11.1 | This command was introduced. | | | | |

Example

This example shows how to display the tunnel manager statistics for a specific WNCd instance:

```
Device# show tunnel eogre manager stats instance 0

Tunnel Manager statistics for process instance : 0
Last Updated                               : 02/18/2019 23:50:35
EoGRE Objects
  Gateways                                  : 6
  Domains                                    : 2

EoGRE Flex Objects
  AP Gateways                               : 2
  AP Domains                                 : 1
  AP Gateways HA inconsistencies            : 0
  AP Domains HA inconsistencies            : 0

Config events
  IOS Tunnel updates                        : 102
  IOS Domain updates                        : 11
  Global updates                            : 6
  Tunnel Profile updates                    : 15
  Tunnel Rule updates                       : 2
  AAA proxy key updates                     : 0

AP events
  Flex AP Join                              : 1
  Flex AP Leave                              : 0
  Local AP Join                             : 0
  Local AP leave                             : 0
  Tunnel status (rx)                        : 4
  Domain status (rx)                        : 1
  IAPP stats msg (rx)                       : 3
  Client count (rx)                         : 6
  VAP Payload msg (tx)                      : 4
```

show tunnel eogre manager stats instance

```

Domain config (tx)           : 1
Global config (tx)          : 1
Client delete (tx)          : 1
Client delete per domain (tx) : 3
DHCP option 82 (tx)         : 4

Client events
Add-mobile                  : 2
Run-State                   : 3
Delete                      : 1
Cleanup                     : 0
Join                        : 2
Plumb                       : 0
Join Errors                 : 0
HandOff                     : 0
MsPayload                   : 2
FT Recover                  : 0
Zombie GW counter increase  : 0
Zombie GW counter decrease  : 0
Tunnel Profile reset        : 11
Client deauth               : 0
HA reconciliation           : 0

Client Join Events
Generic Error               : 0
MSPayload Fail              : 0
Invalid VLAN                : 0
Invalid Domain              : 0
No GWs in Domain            : 0
Domain Shut                 : 0
Invalid GWs                 : 0
GWs Down                    : 0
Rule Match Error            : 0
AAA-override                : 0
Flex No Active GW           : 0
Open Auth join attempt      : 2
Dot1x join attempt          : 2
Mobility join attempt       : 0
Tunnel Profile not valid    : 2
Tunnel Profile valid        : 2
No rule match               : 0
Rule match                   : 2
AAA proxy                   : 0
AAA proxy accounting        : 0
AAA eogre attributes        : 0
Has aaa override            : 0
Error in handoff payload    : 0
Handoff AAA override        : 0
Handoff no AAA override     : 0
Handoff payload received    : 0
Handoff payload sent        : 0

SNMP Traps
Client                      : 0
Tunnel                      : 2
Domain                      : 0

IPC
IOSd TX messages            : 0

Zombie Client
Entries                     : 0

```

show umbrella config

To view the Umbrella configuration details, use the **show umbrella config** command.

show umbrella config

| | | |
|---------------------------|--------------------------------|------------------------------|
| Syntax Description | This command has no arguments. | |
| Command Default | None | |
| Command Modes | Global configuration | |
| Command History | Release | Modification |
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the Umbrella configuration details:

```
Device# show umbrella config
Umbrella Configuration
=====
Token: 57CC80106C087FB1B2A7BAB4F2F4373C00247166
OrganizationID: 1892929
Local Domain Regex parameter-map name: dns_wl
DNSCrypt: Enabled
Public-key: B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79

UDP Timeout: 2 seconds
Resolver address:
 1. 208.67.220.220
 2. 208.67.222.222
 3. 2620:119:53::53
 4. 2620:119:35::35
```

show umbrella deviceid

To view the device registration details, use the **show umbrella deviceid** command.

show umbrella deviceid

| | |
|---------------------------|--------------------------------|
| Syntax Description | This command has no arguments. |
|---------------------------|--------------------------------|

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

| | |
|----------------------|----------------------|
| Command Modes | Global configuration |
|----------------------|----------------------|

| Command History | Release | Modification |
|------------------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the device registration details:

```
Device# show umbrella deviceid
Device registration details
Profile Name          Tag          Status          Device-id
GigabitEthernet0/0/0  guest       200 SUCCESS     010a470b042a072d
```


show umbrella deviceid detailed

To view the detailed description for the Umbrella device ID, use the **show umbrella deviceid detailed** command.

show umbrella deviceid *detailed*

| Syntax Description | This command has no arguments. | | | | |
|--------------------------------|--|---------|--------------|--------------------------------|------------------------------|
| Command Default | None | | | | |
| Command Modes | Global configuration | | | | |
| Command History | <table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>Cisco IOS XE Gibraltar 16.10.1</td><td>This command was introduced.</td></tr></tbody></table> | Release | Modification | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. | | | | |

This example shows how to view the detailed description for the Umbrella device ID:

```
Device# show umbrella deviceid detailed
Device registration details
 1.GigabitEthernet0/0/0
   Tag           : guest
   Device-id     : 010a470b042a072d
   Description   : Device Id recieved successfully
```

show umbrella dnscrypt

To view the Umbrella DNSCrypt details, use the **show umbrella dnscrypt** command.

show umbrella dnscrypt

| | | |
|---------------------------|--------------------------------|------------------------------|
| Syntax Description | This command has no arguments. | |
| Command Default | None | |
| Command Modes | Global configuration | |
| Command History | Release | Modification |
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the Umbrella DNSCrypt details:

```
Device# show umbrella dnscrypt
DNSCrypt: Enabled
Public-key: B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8DOC:BE04:BFAB:CA43:FB79

Certificate Update Status:
  Last Successfull Attempt: 17:45:57 IST Nov 9 2017
Certificate Details:
Certificate Magic      : DNSC
Major Version         : 0x0001
Minor Version         : 0x0000
Query Magic           : 0x713156774457306E
Serial Number         : 1490391488
Start Time            : 1490391488 (03:08:08 IST Mar 25 2017)
End Time              : 1521927488 (03:08:08 IST Mar 25 2018)
Server Public Key     :
E7F8:4477:BF89:1434:1ECE:23F0:D6A6:6EB9:4F45:3167:D71F:80BB:4E80:A04F:F180:F778
Client Secret Key Hash:
F1A5:1993:F729:5416:53B7:94E3:6509:8182:A708:0561:8050:6CE0:DFA1:5C94:6EE4:0010
Client Public key     :
BC6D:3758:48B6:120B:D2F5:F25B:2979:564D:F52C:5EFA:B0BD:76FE:3CD6:828B:44D2:FF3A
NM key Hash           :
1FF7:2E1E:EFB9:7987:9CB4:3EF8:A25B:4DAD:10FC:7DF7:6985:6E8E:6E4D:D56A:1C70:B9EB
```

show vlan

To display the parameters for all configured VLANs or one VLAN (if the VLAN ID or name is specified) on the switch, use the **show vlan** command in user EXEC mode.

```
show vlan [{brief | group | id vlan-id | mtu | name vlan-name | remote-span | summary}]
```

| Syntax | Description |
|------------------------------|---|
| brief | (Optional) Displays one line for each VLAN with the VLAN name, status, and its ports. |
| group | (Optional) Displays information about VLAN groups. |
| id <i>vlan-id</i> | (Optional) Displays information about a single VLAN identified by the VLAN ID number. For <i>vlan-id</i> , the range is 1 to 4094. |
| mtu | (Optional) Displays a list of VLANs and the minimum and maximum transmission unit (MTU) sizes configured on ports in the VLAN. Note Traceback occurs in the VLAN CLI parser when Controller-PI does VLAN lookup for each interface. |
| name <i>vlan-name</i> | (Optional) Displays information about a single VLAN identified by the VLAN name. The VLAN name is an ASCII string from 1 to 32 characters. |
| remote-span | (Optional) Displays information about Remote SPAN (RSPAN) VLANs. |
| summary | (Optional) Displays VLAN summary information. |



Note The **ifindex** keyword is not supported, even though it is visible in the command-line help string.

Command Default None

Command Modes User EXEC

| Command History | Release | Modification |
|-----------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

Usage Guidelines In the **show vlan mtu** command output, the MTU_Mismatch column shows whether all the ports in the VLAN have the same MTU. When yes appears in the column, it means that the VLAN has ports with different MTUs, and packets that are switched from a port with a larger MTU to a port with a smaller MTU might be dropped. If the VLAN does not have an SVI, the hyphen (-) symbol appears in the SVI_MTU column. If the MTU-Mismatch column displays yes, the names of the ports with the MinMTU and the MaxMTU appear.

This is an example of output from the **show vlan** command. See the table that follows for descriptions of the fields in the display.

```

Device> show vlan
VLAN Name                               Status    Ports
-----
1    default                               active   Gi1/0/2, Gi1/0/3, Gi1/0/4
                                           Gi1/0/5, Gi1/0/6, Gi1/0/7
                                           Gi1/0/8, Gi1/0/9, Gi1/0/10
                                           Gi1/0/11, Gi1/0/12, Gi1/0/13
                                           Gi1/0/14, Gi1/0/15, Gi1/0/16
                                           Gi1/0/17, Gi1/0/18, Gi1/0/19
                                           Gi1/0/20, Gi1/0/21, Gi1/0/22
                                           Gi1/0/23, Gi1/0/24, Gi1/0/25
                                           Gi1/0/26, Gi1/0/27, Gi1/0/28
                                           Gi1/0/29, Gi1/0/30, Gi1/0/31
                                           Gi1/0/32, Gi1/0/33, Gi1/0/34
                                           Gi1/0/35, Gi1/0/36, Gi1/0/37
                                           Gi1/0/38, Gi1/0/39, Gi1/0/40
                                           Gi1/0/41, Gi1/0/42, Gi1/0/43
                                           Gi1/0/44, Gi1/0/45, Gi1/0/46
                                           Gi1/0/47, Gi1/0/48

2    VLAN0002                               active
40   vlan-40                                 active
300  VLAN0300                               active
1002 fddi-default                          act/unsup
1003 token-ring-default                   act/unsup
1004 fddinet-default                      act/unsup
1005 trnet-default                        act/unsup

VLAN Type  SAID      MTU   Parent  RingNo  BridgeNo  Stp   BrdgMode  Trans1  Trans2
-----
1    enet     100001    1500  -       -       -       -       -       0       0
2    enet     100002    1500  -       -       -       -       -       0       0
40   enet     100040    1500  -       -       -       -       -       0       0
300  enet     100300    1500  -       -       -       -       -       0       0
1002 fddi     101002    1500  -       -       -       -       -       0       0
1003 tr       101003    1500  -       -       -       -       -       0       0
1004 fdnet   101004    1500  -       -       -       ieee    -       0       0
1005 trnet   101005    1500  -       -       -       ibm     -       0       0
2000 enet     102000    1500  -       -       -       -       -       0       0
3000 enet     103000    1500  -       -       -       -       -       0       0

Remote SPAN VLANs
-----
2000,3000

Primary Secondary Type                Ports
-----

```

Table 15: show vlan Command Output Fields

| Field | Description |
|--------|---|
| VLAN | VLAN number. |
| Name | Name, if configured, of the VLAN. |
| Status | Status of the VLAN (active or suspend). |
| Ports | Ports that belong to the VLAN. |

| Field | Description |
|-------------------|---|
| Type | Media type of the VLAN. |
| SAID | Security association ID value for the VLAN. |
| MTU | Maximum transmission unit size for the VLAN. |
| Parent | Parent VLAN, if one exists. |
| RingNo | Ring number for the VLAN, if applicable. |
| BrdgNo | Bridge number for the VLAN, if applicable. |
| Stp | Spanning Tree Protocol type used on the VLAN. |
| BrdgMode | Bridging mode for this VLAN—possible values are source-route bridging (SRB) and source-route transparent (SRT); the default is SRB. |
| Trans1 | Translation bridge 1. |
| Trans2 | Translation bridge 2. |
| Remote SPAN VLANs | Identifies any RSPAN VLANs that have been configured. |

This is an example of output from the **show vlan summary** command:

```
Device> show vlan summary
Number of existing VLANs           : 45
Number of existing VTP VLANs      : 45
Number of existing extended VLANs : 0
```

This is an example of output from the **show vlan id** command:

```
Device# show vlan id 2
VLAN Name                Status      Ports
-----
2    VLAN0200                active     Gi1/0/7, Gi1/0/8
2    VLAN0200                active     Gi2/0/1, Gi2/0/2

VLAN Type  SAID      MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
-----
2    enet  100002   1500  -     -     -     -     -     0     0

Remote SPAN VLANs
-----
Disabled
```

show vlan access-map

To display information about a particular VLAN access map or for all VLAN access maps, use the **show vlan access-map** command in privileged EXEC mode.

```
show vlan access-map [map-name]
```

| | | |
|---------------------------|--|------------------------------|
| Syntax Description | <i>map-name</i> (Optional) Name of a specific VLAN access map. | |
| Command Default | None | |
| Command Modes | Privileged EXEC | |
| Command History | Release | Modification |
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This is an example of output from the **show vlan access-map** command:

```
Device# show vlan access-map
Vlan access-map "vmap4" 10
  Match clauses:
    ip address: a12
  Action:
    forward
Vlan access-map "vmap4" 20
  Match clauses:
    ip address: a12
  Action:
    forward
```

show vlan filter

To display information about all VLAN filters or about a particular VLAN or VLAN access map, use the **show vlan filter** command in privileged EXEC mode.

```
show vlan filter {access-map name | vlan vlan-id}
```

| Syntax Description | access-map <i>name</i> (Optional) Displays filtering information for the specified VLAN access map. | | | | |
|--------------------------------|--|---------|--------------|--------------------------------|------------------------------|
| | vlan <i>vlan-id</i> (Optional) Displays filtering information for the specified VLAN. The range is 1 to 4094. | | | | |
| Command Default | None | | | | |
| Command Modes | Privileged EXEC | | | | |
| Command History | <table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>Cisco IOS XE Gibraltar 16.10.1</td><td>This command was introduced.</td></tr></tbody></table> | Release | Modification | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. | | | | |

This is an example of output from the **show vlan filter** command:

```
Device# show vlan filter
VLAN Map map_1 is filtering VLANs:
 20-22
```

show vlan group

To display the VLANs that are mapped to VLAN groups, use the **show vlan group** command in privileged EXEC mode.

```
show vlan group [{group-name vlan-group-name [user_count]]
```

Syntax Description

group-name *vlan-group-name* (Optional) Displays the VLANs mapped to the specified VLAN group.

user_count (Optional) Displays the number of users in each VLAN mapped to a specified VLAN group.

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

The **show vlan group** command displays the existing VLAN groups and lists the VLANs and VLAN ranges that are members of each VLAN group. If you enter the **group-name** keyword, only the members of the specified VLAN group are displayed.

This example shows how to display the members of a specified VLAN group:

show vrrp events

To display Virtual Router Redundancy Protocol (VRRP) events, use the **show vrrp events** command.

show vrrp events

| | |
|---------------------------|--|
| Syntax Description | This command has no keywords or arguments. |
|---------------------------|--|

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

| | |
|----------------------|--------------------|
| Command Modes | Privileged EXEC(#) |
|----------------------|--------------------|

| Command History | Release | Modification |
|------------------------|-------------------------------|------------------------------|
| | Cisco IOS XE Amsterdam 17.2.1 | This command was introduced. |

| | |
|-------------------------|--|
| Usage Guidelines | VRRP commands are displayed only in ME mode; it is hidden in other AP modes. |
|-------------------------|--|

Examples

This example shows how to view the VRRP events:

```
Device# show vrrp events
```

```
VRRP Events:
Dec 7 2019 01:17:23: Current state : backup, My Eth : A4:53:0E:7B:CD:84, event : VRRP Element
  is started. Start
  sending KeepAlive Pkts to check if Ether link is up
Dec 7 2019 01:17:28: Current state : backup, My Eth : A4:53:0E:7B:CD:84, event : Detected
  Link is up. Now
  waiting for 30 seconds to participate in VRRP election
Dec 7 2019 01:18:01: Current state : master, My Eth : A4:53:0E:7B:CD:84, event : Current
  master
  (00:00:00:00:00:00) went down (lost 3 advertisement). Moving to master state. And starting
  election
Dec 7 2019 01:18:05: Current state : master, My Eth : A4:53:0E:7B:CD:84, event : Launched
  controller process on
  this ap
```

show vrrp statistics

To display the Virtual Router Redundancy Protocol (VRRP) statistics, use the **show vrrp statistics** command in privileged EXEC mode.

show vrrp statistics

| | | |
|---------------------------|--|------------------------------|
| Syntax Description | This command has no keywords or arguments. | |
| Command Default | None | |
| Command Modes | Privileged EXEC (#) | |
| Command History | Release | Modification |
| | Cisco IOS XE Amsterdam 17.2.1 | This command was introduced. |
| Usage Guidelines | VRRP commands are displayed only in ME mode; it is hidden in other AP modes. | |

Examples

This example shows how to view the VRRP statistics:

```
Device# show vrrp statistics

VRRP Statistics :
VRRP Statistics :
Invalid VRRP packets recvd:0
Number of incoming VRRP Pkts:0
Number of VRRP Pkts transmitted:148054
Number of VRRP Pkts recvd from Master:0
Number of VRRP Pkts recvd in Init state:0
Number of VRRP Pkts with STOP Priority:0
```

show vrrp status

To display the Virtual Router Redundancy Protocol (VRRP) status, use the **show vrrp status** command.

show vrrp status

| | |
|---------------------------|--|
| Syntax Description | This command has no keywords or arguments. |
|---------------------------|--|

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

| | |
|----------------------|--------------------|
| Command Modes | Privileged EXEC(#) |
|----------------------|--------------------|

| Command History | Release | Modification |
|------------------------|-------------------------------|------------------------------|
| | Cisco IOS XE Amsterdam 17.2.1 | This command was introduced. |

| | |
|-------------------------|--|
| Usage Guidelines | VRRP commands are displayed only in ME mode; it is hidden in other AP modes. |
|-------------------------|--|

Examples

This example shows how to view the VRRP status:

```
Device# show vrrp status

  VRRP Status : MASTER
Preferred AP : 00:00:00:00:00:00
My Eth : A4:53:0E:7B:CD:84
AP Type : VANCOUVER
VRRP Instance : vrid state priority vrrp_ip_vlans adver_ival
1 master 1 0.0.0.0:0 3.000000
```

show wireless afc ap

To check whether Automated Frequency Coordination (AFC) service request can be sent, use the **show wireless afc ap** command.

show wireless afc ap

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC (#)

Command History

| Release | Modification |
|----------------------|------------------------------|
| Cisco IOS XE 17.13.1 | This command was introduced. |

Examples

The following example shows how to check whether the AFC service request can be sent:

```
Device# show wireless afc ap
```

| AP Name | Radio | RF-Profile | Radio MAC | RF-Profile | AFC | AFC Country | Power Mode | Current | AP | 6GHz |
|------------------|-------------|------------|----------------|------------|------------|-------------|-------------|---------|----|------|
| State | Admin State | tx-power | std | allowed | Capability | Power Mode | Admin State | Admin | | |
| APCC9C.3EF1.1620 | | | 10f9.20fe.36a0 | | Inactive | | SP/LPi | LPi | Up | Down |
| Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | | |
| AP687D.B45C.17AC | | | 687d.b45f.1af0 | | Active | | SP/LPi | SP | Up | Up |
| Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | | |
| AP-ARCTIC | | | fc58.9a18.c890 | | Inactive | | SP/LPi | LPi | Up | Up |
| Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | | |

show wireless afc channels

To view the Automated Frequency Coordination (AFC) system's channel information, use the **show wireless afc channels** command.

show wireless afc channels { 20mhz | 40mhz | 80mhz | 160mhz }

| Syntax Description | |
|--------------------|--|
| 20mhz | Displays 20MHz-band channel information. |
| 40mhz | Displays 40MHz-band channel information. |
| 80mhz | Displays 80MHz-band channel information. |
| 160mhz | Displays 1600MHz-band channel information. |

Command Default None

Command Modes Privileged EXEC (#)

| Command History | Release | Modification |
|-----------------|----------------------|------------------------------|
| | Cisco IOS XE 17.13.1 | This command was introduced. |

Examples

The following example shows how to view the AFC system's channel information:

```

Device# show wireless afc channels 20mhz

802.11 6ghz   : 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Channel IDs  : 1 1 2 2 2 3 3 4 4 4 5 5 6 6 6 7 7 8 8 8 9 9 0 0 0
(20MHz width) : 1 5 9 3 7 1 5 9 3 7 1 5 9 3 7 1 5 9 3 7 1 5 9 3 7
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
AP687D.B45C.08F0 : 36 33 36 36 35 36 36 36 26 27 36 36 36 36 36 36 33 33 36 36 36 36 36 36
 36
AP687D.B45C.1824 : 36 33 36 36 35 36 36 36 24 26 27 36 36 36 36 36 33 33 36 36 36 36 36 36
 36

! Due to space constraints, the channel IDs (for 2-digit and 3-digit channel IDs)
! are given vertically in the output. The output is also truncated to fit the page width.
    
```

show wireless afc geolocation

To view the geolocation information of the Automated Frequency Coordination (AFC) system, use the **show wireless afc geolocation** command.

show wireless afc geolocation

| | |
|---------------------------|--|
| Syntax Description | This command has no keywords or arguments. |
|---------------------------|--|

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

| | |
|----------------------|---------------------|
| Command Modes | Privileged EXEC (#) |
|----------------------|---------------------|

| | | |
|------------------------|----------------------|------------------------------|
| Command History | Release | Modification |
| | Cisco IOS XE 17.13.1 | This command was introduced. |

Examples

The following example shows how to view the geolocation information of the AFC system:

```
Device# show wireless afc geolocation
```

| AP Name | Radio MAC | Location | Longitude | Latitude | Major-axis | Minor-axis |
|------------------|----------------|-------------|-------------|-------------|-------------|------------|
| Orientation | Area-of-uncert | Height | Height | Uncertainty | | |
| (degrees) | (sq. meters) | Type | (meters) | (degrees) | (degrees) | (meters) |
| AP687D.B45C.16A4 | 687d.b45f.0e90 | Lin Polygon | -122.400140 | 37.794910 | | |
| | 1122 | AGL | 150 | 6 | | |
| | | | | | -122.399340 | 37.795020 |
| | | | | | -122.399180 | 37.794390 |
| | | | | | -122.400040 | 37.794270 |
| AP687D.B45C.17AC | 687d.b45f.1af0 | Ellipse | -73.977760 | 40.760168 | 9 | 9 |
| | 5.340000 | AGL | 129 | 3 | | |

! The afc geolocation information given in the output refers to coordinates to be used for future AFC requests.

! They do not represent the coordinates used by past AFC requests; for such info see AFC responses in 'show wireless afc response' command.

```
.
.
.
```

show wireless afc request

To view the status of the request sent to the Automated Frequency Coordination (AFC) system, use the **show wireless afc request** command.

show wireless afc request

| | |
|---------------------------|--|
| Syntax Description | This command has no keywords or arguments. |
|---------------------------|--|

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

| | |
|----------------------|---------------------|
| Command Modes | Privileged EXEC (#) |
|----------------------|---------------------|

| | | |
|------------------------|----------------------|------------------------------|
| Command History | Release | Modification |
| | Cisco IOS XE 17.13.1 | This command was introduced. |

Examples

The following example shows how to view the status request information sent to the AFC system:

```
Device# show wireless afc request
```

```
-----
Last AFC Request Sent to AFC Service:
AP Name          Radio MAC      Request Id      AFC Request Status  Status
Timestamp
-----
APCC9C.3EF1.1620 10f9.20fe.36a0 12195125900336565035 Response Received   08/07/2023
13:20:39
AP687D.B45C.17AC 687d.b45f.1af0 12195125900336565037 Response Received   08/07/2023
16:07:01
AP687D.B45C.321B fc58.9a18.c840 12195125900336566836 Sent                 08/07/2023
17:36:11
AP687D.B45C.321F fc58.9a18.c850 12195125900336566832 Timeout              08/07/2023
17:36:08
.
.
.
```

show wireless afc response

To view Automated Frequency Coordination (AFC) system's response to requests, use the **show wireless afc response** command.

show wireless afc response

| | |
|---------------------------|--|
| Syntax Description | This command has no keywords or arguments. |
|---------------------------|--|

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

| | |
|----------------------|---------------------|
| Command Modes | Privileged EXEC (#) |
|----------------------|---------------------|

| | | |
|------------------------|----------------------|------------------------------|
| Command History | Release | Modification |
| | Cisco IOS XE 17.13.1 | This command was introduced. |

Examples

The following example shows how to view the response information of the AFC system:

```
Device# show wireless afc response
```

| AP Name Time | Response Code | Radio MAC | Request Id | Expire Time | Last Rcvd |
|------------------------------|---------------|----------------|------------|---------------------|------------|
| AP687D.B45C.16A4 17:56:29 | SUCCESS | 687d.b45f.0e90 | 1 | 11/14/2021 21:56:29 | 11/14/2021 |
| AP687D.B45C.17AC 17:56:29 | SUCCESS | 687d.b45f.1af0 | 2 | 11/14/2021 21:56:30 | 11/14/2021 |
| AP687D.B45C.2276 17:56:29 | INVALID VALUE | 687d.b45f.3190 | 3 | 11/14/2021 21:56:30 | 11/14/2021 |

show wireless afc statistics

To view the Automated Frequency Coordination (AFC) system's statistical information, use the **show wireless afc statistics** command.

show wireless afc statistics

| | |
|---------------------------|--|
| Syntax Description | This command has no keywords or arguments. |
|---------------------------|--|

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

| | |
|----------------------|---------------------|
| Command Modes | Privileged EXEC (#) |
|----------------------|---------------------|

| Command History | Release | Modification |
|------------------------|----------------------|------------------------------|
| | Cisco IOS XE 17.13.1 | This command was introduced. |

Examples

The following example shows how to view the AFC system's statistics information:

```
Device# show wireless afc statistics

Total number of 6GHz APs : 4
Number of APs requiring AFC service : 4
Messages sent to AFC : 229
Successful messages received from AFC : 229
Errored AFC messages : 0
AFC messages pending : 0
Last InquiredChannel message sent:
requestId : 12195125900336565222
AP MAC : 10f9.20fd.54e0
Sent timestamp : 08/09/2023 15:14:20
Last InquiredChannel message received:
requestId : 12195125900336565222
AP MAC : 10f9.20fd.54e0
Received timestamp : 08/09/2023 15:14:21
Minimum response time (ms) : 337
Maximum response time (ms) : 40842
Average response time (ms) : 1315
Health check query : Idle
Health check status : OK
Health check timestamp : 08/09/2023 14:58:50
Number of times health check went down : 0

Health check event history
Timestamp #Times Event State RC Context
-----
08/09/2023 14:58:50.348063 53 Response received OK 0
08/09/2023 14:58:48.271529 58 Scheduled 0 Timer: 3600s
08/09/2023 14:58:48.271507 53 Sent 0
08/07/2023 09:33:55.990412 6 Not sent No token 0
```

show wireless stats ap history

To verify historical statistics of an AP, use the **show wireless stats ap history** command.

show wireless stats ap history

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC#

Command History

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

Examples

This example shows how to verify the statistics of the access point history:

```
Device# show wireless stats ap history
AP Name          Radio MAC      Event      Time          Recent      Disconnect
Reason          Disconnect
Count
Time
Disconnect Reason
Time
```

| | | | | | |
|------------------|----------------|-----------|-------------------|----|----------------|
| APA023.9FD8.EA22 | 40ce.24bf.8ca0 | Joined | 06/26/21 10:11:52 | NA | NA |
| NA | | | | | |
| APA023.9FD8.EA22 | 40ce.24bf.8ca0 | Disjoined | 06/26/21 10:05:18 | NA | Heart beat |
| timer expiry 1 | | | | | |
| APA023.9FD8.EA22 | 40ce.24bf.8ca0 | Joined | 06/22/21 17:00:39 | NA | NA |
| NA | | | | | |
| APA023.9FD8.EA22 | 40ce.24bf.8ca0 | Disjoined | 06/22/21 16:54:54 | NA | Heart beat |
| timer expiry 1 | | | | | |
| APA023.9FD8.EA22 | 40ce.24bf.8ca0 | Joined | 06/21/21 23:01:17 | NA | NA |
| NA | | | | | |
| APA023.9FD8.EA22 | 40ce.24bf.8ca0 | Disjoined | 06/21/21 22:56:21 | NA | Image Download |
| Success 1 | | | | | |

show wireless stats ap join summary

To verify the statistics of the access point join summary, use the **show wireless stats ap join summary** command.

show wireless stats ap join summary

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC(#)

| Command History | Release | Modification |
|-----------------|-------------------------------|------------------------------|
| | Cisco IOS XE Cupertino 17.7.1 | This command was introduced. |

Examples

This example shows how to verify the statistics of the access point join summary:

```
Device# show wireless stats ap join summary
Number of APs: 001
```

| Base MAC | Ethernet MAC | AP Name | IP Address | Status | Last Failure | Phase | Last |
|-------------------|----------------|------------------|------------|--------|--------------|-------|------|
| Disconnect Reason | | | | | | | |
| 002a.1075.47c0 | 002a.104d.c9fc | AP002a.104d.c9fc | 8.9.10.222 | Joined | Run | | High |
| CPU usage | | | | | | | |
| 003a.1475.57c0 | 002a.104d.c9fc | AP003a.144d.59fc | 7.8.09.111 | Joined | Run | | High |
| Memory usage | | | | | | | |

show wireless stats ap join summary sort

To view the sorted wireless statistics access point (AP) join summary, use the **show wireless stats ap join summary sort** command.

show wireless stats ap join summary sort

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC (#)

Command History

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

Usage Guidelines Wireless AP statistics can be sorted in ascending or descending order by AP name.

- Ascending: Displays the ten APs from the bottom.
- Descending: Displays the APs from the top.
- Name: Displays the APs list sorted by name.

Examples

This example shows how to view the sorted wireless statistics AP join summary:

```
Device# show wireless stats ap join summary sort
Number of APs: 8
```

| Base MAC Last Failure | Ethernet MAC Phase | AP Name Last Disconnect | Reason | IP Address | Status |
|----------------------------------|--|----------------------------|-------------------|------------|--------|
| 7872.5dee.4960 Image-Download | 7872.5ded.cb74 Image Download | 4800-abcdefghijklmnopqrstu | vwxyz1 Success | 1.11.22.11 | Joined |
| 10f9.2077.6140 Image-Download | 10f9.2076.2c58 Image Download | 9105-abcdefghijklmnopqrstu | vwxyz1 Success | 1.11.22.11 | Joined |
| 00ee.ab18.bf00 Image-Download | 7069.5a74.9670 Image Download | 9115-abcdefghijklmnopqrstu | vwxyz1 Success | 1.11.22.11 | Joined |
| 1416.9d82.ef40 Image-Download | 2c57.4152.5e60 Image Download | 9130-abcdefghijklmnopqrstu | vwxyz1 Success | 1.11.22.11 | Joined |
| 00d7.8f4e.7040 Config | 002a.1087.d68a DTLS close alert from peer | AP2800 | | 1.11.22.11 | Joined |
| 687d.b45e.3ed0 Image-Download | 687d.b45c.0554 Image Download | AP687D.B45C.0554 | | 1.11.22.11 | Joined |
| 687d.b45e.4c50 Config | 687d.b45c.0674 DTLS close alert from peer | AP687D.B45C.0674 | | 1.11.22.11 | Joined |
| 687d.b45e.53d0 Config | 687d.b45c.0714 DTLS close alert from peer | AP687D.B45C.0714 | | 1.11.22.11 | Joined |

show wireless stat redundancy statistics client-recovery mobilityd

To view the statistics of Mobilityd configuration database, use the **show wireless stat redundancy statistics client-recovery mobilityd** command.

show wireless stat redundancy statistics client-recovery mobilityd

| | | |
|---------------------------|--|------------------------------|
| Syntax Description | This command has no keywords or arguments. | |
| Command Default | None | |
| Command Modes | Privileged EXEC (#) | |
| Command History | Release | Modification |
| | Cisco IOS XE Cupertino 17.7.1 | This command was introduced. |

Examples

The following example shows how to view the statistics of Mobilityd configuration database:

```
Device# show wireless stat redundancy statistics client-recovery mobilityd

Mobility Client Deletion Reason Statistics
-----
Mobility Incomplete State           : 0
Inconsistency in WNCD & Mobility    : 0
Partial Delete                       : 0
General statistics                   :
-----
```

show wireless stat redundancy statistics client-recovery sisf

To view the statistics for Switch Integrated Security Features (SISF) configuration database, use the **show wireless stat redundancy statistics client-recovery sisf** command.

show wireless stat redundancy statistics client-recovery sisf

| | |
|---------------------------|--|
| Syntax Description | This command has no keywords or arguments. |
|---------------------------|--|

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

| | |
|----------------------|---------------------|
| Command Modes | Privileged EXEC (#) |
|----------------------|---------------------|

| Command History | Release | Modification |
|------------------------|-------------------------------|------------------------------|
| | Cisco IOS XE Cupertino 17.7.1 | This command was introduced. |

Examples

The following example shows how to view the statistics for SISF configuration database:

```
Device# show wireless stat redundancy statistics client-recovery sisf
Client SSO statistics for SISF
-----
Number of recreate attempted post switchover      : 0
Number of recreate succeeded post switchover      : 0
Number of recreate failed because of no mac      : 0
Number of recreate failed because of no ip       : 0
Number of ipv4 entry recreate success            : 0
Number of ipv4 entry recreate failed              : 0
Number of ipv6 entry recreate success            : 0
Number of ipv6 entry recreate failed              : 0
Number of partial delete received                : 0
Number of client purge attempted                 : 0
Number of heap and db entry purge success        : 0
Number of purge success for db entry only        : 0
Number of client purge failed                    : 0
Number of garp sent                              : 0
Number of garp failed                            : 0
Number of IP table create callbacks on standby   : 0
Number of IP table modify callbacks on standby   : 0
Number of IP table delete callbacks on standby   : 0
Number of MAC table create callbacks on standby  : 0
Number of MAC table modify callbacks on standby  : 0
Number of MAC table delete callbacks on standby  : 0
```

show wireless stat redundancy client-recovery wncd

To view the redundancy configuration statistics for all the Wireless Network Control Daemon (WNCd) instances, use the **show wireless stat redundancy client-recovery wncd** command.

show wireless stat redundancy client-recovery wncd { *instance-id* | **all** }

| Syntax Description | |
|--------------------|--|
| <i>instance-id</i> | Instance ID. Valid values range from 0 to 7. |
| all | Specifies the statistics for all WNCd instances. |

Command Default None

Command Modes Privileged EXEC (#)

| Command History | Release | Modification |
|-----------------|-------------------------------|------------------------------|
| | Cisco IOS XE Cupertino 17.7.1 | This command was introduced. |

Examples

The following example shows how to view the redundancy configuration statistics for all the WNCd instances:

```
Device# show wireless stat redundancy statistics client-recovery wncd all

Client SSO statistics
-----
No. of Clients                               : 0
No. of Clients recovered successfully         : 0
No. of Clients failed to recover             : 0
No. of Reconcile messages received from AP  : 0
WNCd instance                               : 0
Reconcile messages received from AP         : 0
Reconcile clients received from AP         : 0
Recreate attempted post switchover          : 0
Recreate attempted by SANET                 : 0
Recreate attempted by DOT1x                 : 0
Recreate attempted by SISF                  : 0
Recreate attempted by SVC CO                : 0
Recreate attempted by Unknown module       : 0
Recreate succeeded post switchover          : 0
Recreate Failed post switchover             : 0
Recreate Failure in mmif                    : 0
Recreate Failure in co                      : 0
Recreate Failure in sanet                   : 0
Recreate Failure in authmgr                 : 0
Recreate Failure in dot1x                   : 0
Recreate Failure in mab                     : 0
Recreate Failure in sanet_accounting        : 0
Recreate Failure in sisf                    : 0
Recreate Failure in web auth                : 0
Recreate Failure in lisp                     : 0
Recreate Failure in ipv6                    : 0
Recreate Failure in qos                     : 0
```

show wireless band-select

To display the status of the band-select configuration, use the **show wireless band-select** command in privileged EXEC mode.

show wireless band-select

| | |
|---------------------------|--|
| Syntax Description | This command has no arguments or keywords. |
|---------------------------|--|

| | |
|------------------------|--------------------------------|
| Command Default | No default behavior or values. |
|------------------------|--------------------------------|

| | |
|----------------------|-----------------|
| Command Modes | Privileged EXEC |
|----------------------|-----------------|

| Command History | Release | Modification |
|------------------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

The following is sample output from the **show wireless band-select** command:

```
Device# show wireless band-select
Band Select Probe Response      : per WLAN enabling
Cycle Count                     : 2
Cycle Threshold (millisec)     : 200
Age Out Suppression (sec)      : 20
Age Out Dual Band (sec)        : 60
Client RSSI (dBm)              : 80
```


show wireless certification config

To display the wireless certification configuration summary, use the **show wireless certification config** command.

show wireless certification config

| | |
|---------------------------|--|
| Syntax Description | This command has no keywords or arguments. |
|---------------------------|--|

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

| | |
|----------------------|---------------------|
| Command Modes | Privileged EXEC (#) |
|----------------------|---------------------|

| Command History | Release | Modification |
|------------------------|-----------------------------|------------------------------|
| | Cisco IOS XE Dublin 17.12.1 | This command was introduced. |

Example

This example shows how to display the wireless certification configuration summary:

```
Device# show wireless certification config
Wireless Certification Configurations

WLANCC                               : Not Configured
FIPS                                  : Not Configured

AP DTLS Version                       : DTLS v1.0 - v1.2
AP DTLS Cipher Suite List:

-----
Ciphersuite (Implicit list)
-----
AES128-SHA
DHE-RSA-AES128-SHA
DHE-RSA-AES256-SHA
DHE-RSA-AES256-SHA256
ECDHE-RSA-AES128-GCM-SHA256
ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-ECDSA-AES256-GCM-SHA384
```

The output can vary depending on the various security modes and AP DTLS configurations.

show wireless client

To see the summary of the classified devices, use the **show wireless client** command.

```
show wireless client device {cache | count | summary } | {steering} [{chassis{chassis-number | active | standby }}]R0
```

| Syntax Description | device | Shows classified devices. |
|--------------------|-----------------------|---|
| | steering | Wireless client steering information |
| | cache | Shows the cached classified device summary. |
| | count | Shows the wireless device count. |
| | summary | Shows the active classified device summary. |
| | <i>chassis-number</i> | Chassis number. Valid range is 1–2. |
| | active | Active instance. |
| | standby | Standby instance. |
| | R0 | Route-Processor slot 0. |

Command Default None

Command Modes Privileged EXEC

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

Examples

The following example shows how to see the summary of the classified devices:

```
Device# show wireless client device summary
```

show wireless client mac-address

To view detailed information of a client using its mac-address, use the **show wireless client mac-address detail** command.

show wireless client mac-address *mac-address* **detail** [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

| Syntax Description | |
|-----------------------|-------------------------------------|
| <i>mac-address</i> | Client MAC address. |
| <i>chassis-number</i> | Chassis number. Valid range is 1–2. |
| active | Active instance. |
| standby | Standby instance. |
| R0 | Route-Processor slot 0. |

Command Default None

Command Modes Privileged EXEC (#)

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

Usage Guidelines The Client Scan Reports section in the output of the **show wireless client mac-address detail** is populated only for the following Apple devices:

- Any iPhone 7 and running iOS 11.0 or higher
- Any iPad after iPad Pro (1st gen, 12.9-inch, 2015) and running iOS 11.0 or higher

Other client devices, even if it supports 802.11k or is Wi-Fi Agile Multiband (MBO) certified, are not currently supported to populate the Client Scan Reports section.

Client ACLs shown under **show wireless client mac-address <mac address> detail** are ACLs applied on the client in Flexconnect local authentication case with MAB+Web authentication WLAN with AAA override enabled. This is applicable only for Express Wi-Fi by Facebook Policy on Controller. For more information about Facebook policy, see [Express Wi-Fi by Facebook](#).

From Cisco IOS XE Amsterdam 17.3.1 onwards, the controller retains client session for 10 seconds. This feature is applicable for clients in the RUN state and is supported on central authentication with local and flex mode.

In idle state, 10 sec represents idle state timeout and 09 sec represent remaining time out of 10 sec. An example is given below:

```
Idle state timeout : 10 sec (Remaining time: 09 sec)
```

Examples

The following example shows how to see detailed client information using its MAC address:

```
Device# show wireless client mac-address 98-XX-7B-XX-EF-XX detail
```

show wireless client mac-address (Call Control)

To view call control information related to clients, use the **show wireless client mac-address** command in privileged EXEC mode.

show wireless client mac-address *mac-address* **call-control call-info**

| | | |
|---------------------------|---|--|
| Syntax Description | <i>mac-address</i> | The client MAC address. |
| | call-control call-info | Displays the call control and IP-related information about a client. |
| Command Default | None | |
| Command Modes | Privileged EXEC | |
| Command History | Release | Modification |
| | Cisco IOS XE Gibraltar 16.10.1 This command was introduced. | |

This example shows how to display call control and IP-related information about a client:

```
Device# show wireless client mac-address 30e4.db41.6157 call-control call-info
Client MAC Address      : 30E4DB416157

Call 1 Statistics

Uplink IP Address      : 209.165.200.225
Downlink IP Address    : 209.165.200.226
Uplink Port            : 29052
Downlink Port          : 27538
Call ID                : c40acb4d-3b3b0.3d27dale-356bed03
Called Party           : sip:1011
Calling Party          : sip:1012
Priority                : 6
Call On Hold           : false
Call Duration          : 30

Call 2 Statistics

No Active Call
```

show wireless client mac-address (TCLAS)

To view information about TCLAS and user priority, use the **show wireless client mac-address** command in privileged EXEC mode.

show wireless client mac-address *mac-address* **tclas**

| Syntax Description | |
|--------------------|--|
| <i>mac-address</i> | The client MAC address. |
| tclas | Displays TCLAS and user priority-related information about a client. |

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to display the TCLAS and user priority-related information about a client:

```
Device# show wireless client mac-address 30e4.db41.6157 tclas
MAC Address      UP TID Mask Source IP Addr  Dest IP Addr  SrcPort DstPort Proto
-----
30e4.db41.6157   4  4  95 167838052      2164326668    5060     5060     6
30e4.db41.6157   6  1  31 0              2164326668    0        27538    17
```

show wireless client mac-address mobility history

To see roam history of an active client in subdomain, use the **show wireless client mac-address *mac-address* mobility history** command.

show wireless client mac-address *mac-address* mobility history [{**chassis** {*chassis-number* | **active** | **standby**} **R0**] | **events** [**chassis** {*chassis-number* | **active** | **standby**} **R0**]]

Syntax Description

| | |
|-----------------------|---|
| <i>mac-address</i> | MAC address of the client. |
| <i>chassis-number</i> | Chassis number as either 1 or 2. |
| active R0 | Active instance of the client in Route-processor slot 0. |
| standby R0 | Standby instance of the client in Route-processor slot 0. |
| events | Shows client FSM event history. |

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Examples

This example shows how to see roam history of an active client in subdomain:

```
Device# show wireless client mac-address 00:0d:ed:dd:35:80 mobility history
```

show wireless client mac-address stats latency

To view a wireless client's statistics using the client's MAC address, use the **show wireless client mac-address mac-address stats latency** command.

```
show wireless client mac-address mac-address stats latency [ chassis { chassis-number | active | standby } R0 ]
```

Syntax Description

| | |
|-----------------------|--|
| <i>mac-address</i> | Client MAC address. |
| stats | Specifies the statistics of the wireless client's MAC address. |
| latency | Specifies the latency statistics of the wireless client's MAC address. |
| chassis | Specifies the chassis for statistics latency. |
| <i>chassis-number</i> | Chassis number, which can be either 1 or 2. |
| active | Specifies an active instance. |
| standby | Specifies a standby instance. |
| R0 | Specifies the route processor for Slot 0. |

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

| Release | Modification |
|-----------------------------|------------------------------|
| Cisco IOS XE Dublin 17.11.1 | This command was introduced. |

Examples

The following example shows how to view the statistics of a wireless client using its MAC address:

```
Device# show wireless client mac-address aaaa.bbbb.cccc stats latency
```


show wireless client summary

To display a summary of active clients associated with the controller, use the **show wireless client summary** command in privileged EXEC mode.

show wireless client summary

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

Usage Guidelines The following is sample output from the **show wireless client summary** command:
Use the **show wireless exclusionlist** command to display clients on the exclusion list.

```
Device# show wireless client summary
```

```
Number of Clients: 1
```

| MAC Address | AP Name | Type ID | State | Protocol | Method | Role |
|----------------|-----------------------|---------|-------|----------|--------|-------|
| 6c40.0899.0466 | 9115i-r4-sw2-te1-0-37 | WLAN 7 | Run | 11ac | None | Local |

show wireless client timers

To display 802.11 system timers, use the **show wireless client timers** command in privileged EXEC mode.

show wireless client timers

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

The following is sample output from the **show wireless client timers** command:

```
Device# show wireless client timers
Authentication Response Timeout (seconds)      : 10
```

show wireless country

To display the configured country and the radio types supported, use the **show wireless country** command in privileged EXEC mode.

show wireless country {channels | configured | supported [tx-power]}

| | | |
|---------------------------|--------------------------------|---|
| Syntax Description | channels | Displays the list of possible channels for each band, and the list of channels allowed in the configured countries. |
| | configured | Display configured countries. |
| | supported tx-power | Displays the list of allowed Tx powers in each supported country. |
| Command Default | No default behavior or values. | |
| Command Modes | Privileged EXEC | |
| Command History | Release | Modification |
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

The following is sample output from the **show wireless country channels** command:

```

Device# show wireless country channels
  Configured Country.....: US - United States
  KEY: * = Channel is legal in this country and may be configured manually.
       A = Channel is the Auto-RF default in this country.
       . = Channel is not legal in this country.
       C = Channel has been configured for use by Auto-RF.
       x = Channel is available to be configured for use by Auto-RF.
       (-,-) = (indoor, outdoor) regulatory domain allowed by this country.
-----:+++++-----
      802.11bg      :
      Channels      :          1 1 1 1 1
                    : 1 2 3 4 5 6 7 8 9 0 1 2 3 4
-----:+++++-----
(-A , -AB ) US   : A * * * * A * * * * A . . .
Auto-RF          : . . . . .
-----:+++++-----
      802.11a      :
      Channels      :          1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
                    : 3 3 3 4 4 4 4 4 4 5 5 6 6 0 0 0 1 1 2 2 3 3 4 4 5 5 6 6
                    : 4 6 8 0 2 4 6 8 2 6 0 4 0 4 8 2 6 0 4 8 2 6 0 9 3 7 1 5
-----:+++++-----
(-A , -AB ) US   : . A . A . A . A A A A A * * * * * . . . * * * A A A A *
Auto-RF          : . . . . .
-----:+++++-----
      4.9GHz 802.11a :
      Channels      :          1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2
                    : 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6
-----:+++++-----
US (-A , -AB ) : * * * * * * * * * * * * * * * A * * * * * A
Auto-RF        : . . . . .
-----:+++++-----

```



```
(-I , -I ) ILO : . . . . 20 20 20 20 20 20 20 20 20 20 20 .
(-A , -AN ) IN : 27 27 27 27 27 27 27 27 27 27 27 . . .
(-E , -E ) IQ : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) IS : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) IT : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-JPU , -JPU ) J2 : 23 23 23 23 23 23 23 23 23 23 23 23 23 23
(-JPU , -JPU ) J3 : 23 23 23 23 23 23 23 23 23 23 23 23 23 23
(-JPQU , -PQ ) J4 : 23 23 23 23 23 23 23 23 23 23 23 23 23 23
(-E , - ) JO : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-JPU , -JPU ) JP : 23 23 23 23 23 23 23 23 23 23 23 23 23 23
(-ACE , -ACEK) KE : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) KN : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-ACE , -ACEK) KR : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) KW : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) KZ : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) LB : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) LI : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , - ) LK : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) LT : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) LU : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) LV : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) MC : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) ME : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) MK : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , - ) MO : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) MT : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-A , -NA ) MX : 27 27 27 27 27 27 27 27 27 27 27 27 . . .
(-ACE , -AEC ) MY : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) NL : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) NO : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-A , -NA ) NZ : 27 27 27 27 27 27 27 27 27 27 27 27 . . .
(-E , -E ) OM : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-A , -AR ) PA : 27 27 27 27 27 27 27 27 27 27 27 27 . . .
(-A , -AR ) PE : 27 27 27 27 27 27 27 27 27 27 27 27 . . .
(-A , -ABN ) PH : 27 27 27 27 27 27 27 27 27 27 27 27 . . .
(-A , -ABN ) PH2 : 27 27 27 27 27 27 27 27 27 27 27 27 . . .
(-E , -E ) PK : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) PL : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-A , -A ) PR : 27 27 27 27 27 27 27 27 27 27 27 27 . . .
(-E , -E ) PT : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-A , -A ) PY : 27 27 27 27 27 27 27 27 27 27 27 27 . . .
(-E , -E ) QA : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) RO : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) RS : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-AER , -ER ) RU : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-AE , -AE ) SA : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) SE : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -SE ) SG : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-E , -E ) SI : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) SK : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -ER ) TH : 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) TN : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-EI , -E ) TR : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-A , -ANT ) TW : 27 27 27 27 27 27 27 27 27 27 27 27 . . .
(-E , -E ) UA : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-A , -AB ) US : 27 27 27 27 27 27 27 27 27 27 27 27 . . .
(-A , -AB ) US2 : 27 27 27 27 27 27 27 27 27 27 27 27 . . .
(-A , -AB ) USL : 27 27 27 27 27 27 27 27 27 27 27 27 . . .
(-A , - ) USX : 27 27 27 27 27 27 27 27 27 27 27 27 . . .
(-A , -A ) UY : 27 27 27 27 27 27 27 27 27 27 27 27 . . .
(-A , -AR ) VE : 27 27 27 27 27 27 27 27 27 27 27 27 . . .
(-E , -E ) VN : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) ZA : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
```

show wireless detail

To display the details of the wireless parameters configured, use the **show wireless detail** command in privileged EXEC mode.

show wireless detail

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

Usage Guidelines The following parameters are displayed:

- The wireless user idle timeout
- The controller configured RF group name
- Fast SSID change

The following is sample output from the **show wireless detail** command:

```
Device# show wireless detail
User Timeout           : 300
RF network             : default
Fast SSID              : Disabled
```

show wireless dhcp relay statistics

To configure the wireless DHCP relay on the AP, use the **show wireless dhcp relay statistic** command.

show wireless dhcp relay statistic

| | | |
|---------------------------|---|------------------------------|
| Syntax Description | <i>A.B.C.D</i> Indicates the target IPv4 address. | |
| Command Default | None | |
| Command Modes | Privileged EXEC (#) | |
| Command History | Release | Modification |
| | Cisco IOS XE Gibraltar 17.3.1 | This command was introduced. |

Examples

The following example shows how to configure the wireless DHCP relay on the AP:

```
Device# show wireless dhcp relay statistics ip-address 10.1.1.1
```

show wireless dot11h

To see 802.11h configuration details, use the **show wireless dot11h** command.

show wireless dot11h [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

Syntax Description

chassis-number Chassis number. Valid range is 1–2.

active Active instance.

standby Standby instance.

R0 Route-Processor slot 0.

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Examples

The following example shows how to see the 802.11h configuration details:

```
Device# show wireless dot11h
```


show wireless dtls connections

To display the Datagram Transport Layer Security (DTLS) server status, use the **show wireless dtls connections** command in privileged EXEC mode.

show wireless dtls connections

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

The following is sample output from the **show wireless dtls connections** command:

```
Device# show wireless dtls connections
AP Name          Local Port  Peer IP      Peer Port  Ciphersuite
-----
AP-2             Capwap_Ctrl 10.0.0.16   52346     TLS_RSA_WITH_AES_128_CBC_SHA
AP-3             Capwap_Ctrl 10.0.0.17   52347     TLS_RSA_WITH_AES_128_CBC_SHA
```

show wireless exclusionlist

To see the wireless exclusion list, use the **show wireless exclusionlist** command.

show wireless exclusionlist [{**client mac-address** *client-mac-addr* **detail** }] [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

Syntax Description

client-mac-addr Client MAC address.

chassis-number Enter the chassis number as either 1 or 2.

active R0 Active instance of the configuration in Route-processor slot 0.

standby R0 Standby instance of the configuration in Route-processor slot 0.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

| Release | Modification |
|--------------------------------|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |
| Cisco IOS XE Cupertino 17.9.1 | The output of the command was modified to include ARP activity information. |

Examples

The following example shows how to see the wireless exclusion list:

```
Device# show wireless exclusionlist
```

```
Excluded Clients
```

| MAC Address | Description | Exclusion Reason | Time Remaining |
|----------------|-------------|-----------------------|----------------|
| 10da.4320.cce9 | | Client Policy failure | 59 |

The following example shows the exclusion reason for the clients, which has changed from *Client Policy failure* to *Excess ARP activity* from Cisco IOS XE Cupertino 17.9.x onwards:

```
Device# show wireless exclusionlist
```

| MAC Address | Description | Exclusion Reason | Time Remaining |
|----------------|-------------|---------------------|----------------|
| 6c96.cff2.889a | | Excess ARP activity | 53 |

show wireless exclusionlist client mac-address detail

To see the detailed information for active clients, use the **show wireless exclusionlist client mac-address detail** command.

show wireless exclusionlist client mac-address *client-mac-addr* **detail**

| Syntax Description | <i>client-mac-addr</i> Client MAC address. | | | | | | |
|--------------------------------|--|---------|--------------|--------------------------------|---|-------------------------------|---|
| Command Default | None | | | | | | |
| Command Modes | Privileged EXEC (#) | | | | | | |
| Command History | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.10.1</td> <td>This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td> </tr> <tr> <td>Cisco IOS XE Cupertino 17.9.1</td> <td>The output of the command was modified to include ARP activity information.</td> </tr> </tbody> </table> | Release | Modification | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. | Cisco IOS XE Cupertino 17.9.1 | The output of the command was modified to include ARP activity information. |
| Release | Modification | | | | | | |
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. | | | | | | |
| Cisco IOS XE Cupertino 17.9.1 | The output of the command was modified to include ARP activity information. | | | | | | |

Examples

The following example shows how to see the detailed information for active clients:

```
Device# show wireless exclusionlist client mac-address 12da.4820.cce9 detail

Client State : Excluded
Client MAC Address : 12da.4820.cce9
Client IPv4 Address: 20.20.20.6
Client IPv6 Address: N/A
Client Username: N/A
Exclusion Reason : Client Policy failure
Authentication Method : None
Protocol: 802.11ac
AP MAC Address : 58ac.780e.08f0
AP Name: charlie2
AP slot : 1
Wireless LAN Id : 2
Wireless LAN Name: mhe-ewlc
VLAN Id : 20
```

The following example shows how to see the detailed information for active clients, where ARP rate limit exclusion that has changed from *Client Policy failure* to *Excess ARP activity* from Cisco IOS XE Cupertino 17.9.x onwards is shown:

```
Device# show wireless exclusionlist client mac-address 6c96.cff2.889a detail

Client State : Excluded
Client MAC Address : 6c96.cff2.889a
Client IPv4 Address: N/A
Client IPv6 Address: N/A
Client Username: N/A
Exclusion Reason : Excess ARP activity
```

show wireless exclusionlist client mac-address detail

```
Authentication Method : None
Protocol: 802.11ac
AP MAC Address : 4001.7aca.5680
AP Name: AP40CE.2485.D5E8
AP slot : 1
Wireless LAN Id : N/A
VLAN Id : 63
```

show wireless fabric summary

To view the fabric status, use the **show wireless fabric summary** command.

show wireless fabric summary

| | |
|---------------------------|--------------------------------|
| Syntax Description | This command has no arguments. |
|---------------------------|--------------------------------|

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

| | |
|----------------------|----------------------|
| Command Modes | Global configuration |
|----------------------|----------------------|

| Command History | Release | Modification |
|------------------------|--------------------------------|---|
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |
| | Cisco IOS XE 17.14.1 | The output of the command was modified to include IPv6 address. |

This example shows how to view fabric status:

```
Device# show wireless fabric summary
Fabric Status      : Enabled
```

```
Control-plane:
Name                IP-address          Key                  Status
-----
test-map            10.12.13.14         test1                Down
```

```
Fabric VNID Mapping:
Name                L2-VNID             L3-VNID             IP Address           Subnet
Control plane name
-----
test1                12                  10                  10.6.8.9             255.255.255.236
test2
```

This example shows how to view fabric status for IPv6:

```
Device#
Fabric Status      : Enabled
```

```
Control-plane:
Name                IP-address          Key                  Status
-----
test-cp            1100:10:10:10:1:1:1:6  ciscoeca            Up
```

```
Fabric VNID Mapping:
Name                L2-VNID             L3-VNID             IP Address           Subnet
Control plane name
-----
fab-ap              8188                4097                1100:10:10:10::1
ffff:ffff:ffff:ffff:: test-cp
```

show wireless fabric client summary

To see the summary of a fabric enabled wireless client, use the **show wireless fabric client summary** command.

show wireless fabric client summary

Command Default

None

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|--------------------------------|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |
| Cisco IOS XE 17.14.1 | The output of the command was modified to include IPv6 address. |

Examples

The following example shows how to see the fabric enabled wireless client summary:

```
Device# show wireless fabric client summary
```

The following example shows how to see the fabric enabled wireless client summary for IPv6:

```
Device# show wireless fabric client summary
```

```
Number of Fabric Clients : 2
```

| MAC Address | AP Name | Type | ID | State | Protocol | Method |
|----------------|-----------------------|------|----|-------|----------|--------|
| L2 VNID | RLOC IP | | | | | |
| 2c33.7a5b.8fc5 | APC4F7.D54D.0B94 | WLAN | 22 | Run | 11n(2.4) | None |
| 8190 | 1100:10:10:10:1:1:1:6 | | | | | |
| 40ec.995a.434e | APC4F7.D54D.0B94 | WLAN | 20 | Run | 11ac | None |
| 8190 | 1100:10:10:10:1:1:1:6 | | | | | |

show wireless fabric vnid mapping

To view all the VNID mapping details, use the **show wireless fabric vnid mapping** command.

show wireless fabric vnid mapping

Syntax Description

This command has no arguments.

Command Default

None

Command Modes

Global configuration

Command History

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

This example shows how to view all the VNID mapping details:

```
Device# show wireless fabric vnid mapping
Fabric VNID Mapping:
  Name          L2-VNID      L3-VNID      IP Address      Subnet
Control plane name
-----
  test1         12           10           10.6.8.9        255.255.255.236
  test2
```

show wireless flow-control

To display the information about flow control on a particular channel, use the **show wireless flow-control** command in privileged EXEC mode.

show wireless flow-control *channel-id*

| Syntax Description | <i>channel-id</i> Identification number for a channel through which flow control is monitored. | | | | |
|--------------------------------|--|---------|--------------|--------------------------------|------------------------------|
| Command Default | No default behavior or values. | | | | |
| Command Modes | Privileged EXEC | | | | |
| Command History | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.10.1</td> <td>This command was introduced.</td> </tr> </tbody> </table> | Release | Modification | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. | | | | |

The following is sample output from the **show wireless flow-control** *channel-id* command:

```
Device# show wireless flow-control 3
Channel Name           : CAPWAP
FC State               : Disabled
Remote Server State   : Enabled
Pass-thru Mode        : Disabled
EnQ Disabled          : Disabled
Queue Depth           : 2048
Max Retries           : 5
Min Retry Gap (mSec)  : 3
```


show wireless flow-control statistics

To display the complete information about flow control on a particular channel, use the **show wireless flow-control statistics** command in privileged EXEC mode.

show wireless flow-control *channel-id* **statistics**

| Syntax Description | <i>channel-id</i> Identification number for a channel through which flow control is monitored. | | | | |
|--------------------------------|--|---------|--------------|--------------------------------|------------------------------|
| Command Default | No default behavior or values. | | | | |
| Command Modes | Privileged EXEC | | | | |
| Command History | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.10.1</td> <td>This command was introduced.</td> </tr> </tbody> </table> | Release | Modification | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. | | | | |

The following is sample output from the **show wireless flow-control** *channel-id* **statistics** command:

```
Device# show wireless flow-control 3 statistics
Channel Name                : CAPWAP
# of times channel went into FC      : 0
# of times channel came out of FC    : 0
Total msg count received by the FC Infra : 1
Pass-thru msgs send count          : 0
Pass-thru msgs fail count          : 0
# of msgs successfully queued       : 0
# of msgs for which queuing failed  : 0
# of msgs sent thru after queuing   : 0
# of msgs sent w/o queuing          : 1
# of msgs for which send failed     : 0
# of invalid EAGAINS received       : 0
Highest watermark reached           : 0
# of times Q hit max capacity        : 0
Avg time channel stays in FC (mSec)  : 0
```

show wireless load-balancing

To display the status of the load-balancing feature, use the **show wireless load-balancing** command in privileged EXEC mode.

show wireless load-balancing

| | |
|---------------------------|--|
| Syntax Description | This command has no arguments or keywords. |
|---------------------------|--|

| | |
|------------------------|--------------------------------|
| Command Default | No default behavior or values. |
|------------------------|--------------------------------|

| | |
|----------------------|-----------------|
| Command Modes | Privileged EXEC |
|----------------------|-----------------|

| Command History | Release | Modification |
|------------------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

The following is sample output from the **show wireless load-balancing** command:

```
> show wireless load-balancing
Aggressive Load Balancing.....: per WLAN enabling
Aggressive Load Balancing Window (clients).....: 5
Aggressive Load Balancing Denial Count.....: 3

Statistics
Total Denied Count (clients).....: 0
Total Denial Sent (messages).....: 0
Exceeded Denial Max Limit Count (times).....: 0
None 5G Candidate Count (times).....: 0
None 2.4G Candidate Count (times).....: 0
```

show wireless mesh ap fabric summary

To view the mesh AP fabric summary, use the **show wireless mesh ap fabric summary** command.

show wireless mesh ap fabric summary

| | |
|---------------------------|--|
| Syntax Description | This command has no keywords or arguments. |
|---------------------------|--|

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

| | |
|----------------------|---------------------|
| Command Modes | Privileged EXEC (#) |
|----------------------|---------------------|

| Command History | Release | Modification |
|------------------------|-----------------------------|------------------------------|
| | Cisco IOS XE Dublin 17.12.1 | This command was introduced. |

Example

This example shows how to view the mesh AP fabric summary:

```
Device# show wireless mesh ap fabric summary
```

show wireless media-stream client detail

To see the media stream clients information by stream name, use the **show wireless media-stream client detail** command.

show wireless media-stream client detail

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Examples

The following example shows how to see media stream clients information by stream name:

```
Device# show wireless media-stream client detail
```

show wireless media-stream group

To display the wireless media-stream group information, use the **show wireless media-stream group** command.

```
show wireless media-stream group {detail groupName | summary}
```

| Syntax Description | detail groupName | Display media-stream group configuration details of the group mentioned in the command. |
|--------------------|------------------|---|
| | summary | Display media-stream group configuration summary |

Command Default None

Command Modes User EXEC mode or Privileged EXEC mode

Usage Guidelines None.

The following is a sample output of the **show wireless media-stream group detail GRP1** command.

```
Device#show wireless media-stream group detail GRP1
Device#show wireless media-stream group detail GRP1
Media Stream Name : GRP1
Start IP Address : 234.1.1.1
End IP Address : 234.1.1.5
RRC Parameters:
Avg Packet Size(Bytes) : 1200
Expected Bandwidth(Kbps) : 1000
Policy : Admitted
RRC re-evaluation : Initial
QoS : video
Status : Multicast-direct
```

The following is a sample output of the **show wireless media-stream group summary** command.

```
Device#show wireless media-stream group summary
Number of Groups:: 1
Stream Name          Start IP                End IP
Status
-----
GRP1                  234.1.1.1                234.1.1.5
Enabled
```

show wireless media-stream message details

To see the wireless multicast-direct session announcement message details, use the **show wireless media-stream message details** command.

show wireless media-stream message details

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Examples

The following example shows how to see the wireless multicast-direct session announcement message details:

```
Device# show wireless media-stream message details
```

show wireless mobility controller ap

To display the list of access points which have joined the sub-domain, use the **wireless mobility controller ap** command.

show wireless mobility controller ap

| | | |
|---------------------------|----------------------------|---|
| Syntax Description | ap | Show joined Access Point in sub-domain. |
| Command Default | None | |
| Command Modes | Privileged EXEC | |
| Command History | Release | Modification |
| | Cisco IOS XE Denali 16.3.1 | This command was introduced. |
| Usage Guidelines | None | |

This example shows how to list the access points which have joined the sub-domain.

```
Device#show wireless mobility controller ap
Number of AP entries in the sub-domain : 2
```

| AP name | AP radio MAC | Controller IP | Location |
|---------|----------------|---------------|---------------|
| bos2kk | 00f2.8c42.f520 | default-group | default-group |
| IosAP1 | 34ed.522f.7e60 | default-group | default-group |

show wireless media-stream multicast-direct state

To see the state of the wireless multicast-direct configuration, use the **show wireless media-stream multicast-direct state** command.

```
show wireless media-stream multicast-direct state
```

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Examples

The following example shows how to see the state of the wireless multicast-direct configuration:

```
Device# show wireless media-stream multicast-direct state
```


show wireless mesh ap

To see the mesh AP related information, use the **show wireless mesh ap** command.

```
show wireless mesh ap { summary | tree | backhaul } [ chassis { chassis-number | active | standby } R0 ]
```

Syntax Description

| | |
|-----------------------|--|
| summary | Shows the summary of all connected mesh APs. |
| tree | Shows the Mesh AP tree. |
| backhaul | Shows the mesh APs backhaul info. |
| <i>chassis-number</i> | Enter the chassis number as either 1 or 2. |
| active R0 | Active instance of the configuration in Route-processor slot 0. |
| standby R0 | Standby instance of the configuration in Route-processor slot 0. |

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Examples

The following example shows how to see the summary of all the connected mesh APs:

```
Device# show wireless mesh ap summary
```

show wireless mesh ap summary

To see the summary of all connected mesh APs, use the **show wireless mesh ap summary** command.

show wireless mesh ap summary [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

Syntax Description

| | |
|-----------------------|--|
| summary | Shows the summary of all connected mesh APs. |
| <i>chassis-number</i> | Enter the chassis number as either 1 or 2. |
| active R0 | Active instance of the active AP filters in Route-processor slot 0. |
| standby R0 | Standby instance of the active AP filters in Route-processor slot 0. |

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Examples

The following example shows how to see the summary of all connected mesh APs:

```
Device# wireless mesh ap summary
```

show wireless mesh ap tree

To see the mesh AP tree, use the **show wireless mesh ap tree** command.

show wireless mesh ap tree

| | |
|---------------------------|--|
| 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. |

Example

The following example shows how to view the wireless mesh AP tree:

```
Device # show wireless mesh ap tree
```

show wireless mesh ap tree

To see the mesh AP tree, use the **show wireless mesh ap tree** command.

show wireless mesh ap tree

| | |
|---------------------------|--|
| 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. |

Example

The following example shows how to view the wireless mesh AP tree:

```
Device # show wireless mesh ap tree
```

show wireless mesh cac summary

To view the total number of voice calls and bandwidth utilization of APs in the Mesh network, use the **show wireless mesh cac summary** command.

show wireless mesh cac summary

| | |
|---------------------------|--|
| Syntax Description | This command has no keywords or arguments. |
|---------------------------|--|

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

| | |
|----------------------|---------------------|
| Command Modes | Privileged EXEC (#) |
|----------------------|---------------------|

| | | |
|------------------------|--------------------------------|------------------------------|
| Command History | Release | Modification |
| | Cisco IOS XE Gibraltar 16.11.1 | This command was introduced. |

Usage Guidelines

Example

This example shows how to display the total number of voice calls and bandwidth utilization of APs in the Mesh network:

```
Device# show wireless mesh cac summary
```

| AP Name | Slot | Radio | BW Used | Call |
|------------------|------|-----------|---------|------|
| APA023.9FA9.B702 | 0 | 802.11b/g | 0 | 0 |
| | 1 | 802.11a | 0 | 0 |
| APA023.9FA9.D920 | 0 | 802.11b/g | 1140 | 2 |
| | 1 | 802.11a | 0 | 0 |
| AP380E.4DBF.C6A6 | 0 | 802.11b/g | 0 | 0 |
| | 1 | 802.11a | 0 | 0 |
| AP380E.4DBF.C80C | 0 | 802.11b/g | 570 | 0 |
| | 1 | 802.11a | 2144 | 2 |
| AP380E.4DBF.C816 | 0 | 802.11b/g | 0 | 0 |
| | 1 | 802.11a | 0 | 0 |

show wireless mesh config

To see the mesh configurations, use the **show wireless mesh config** command.

show wireless mesh config [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

Syntax Description

| | |
|-----------------------|--|
| config | Shows the mesh configurations. |
| <i>chassis-number</i> | Enter the chassis number as either 1 or 2. |
| active R0 | Active instance of the active AP filters in Route-processor slot 0. |
| standby R0 | Standby instance of the active AP filters in Route-processor slot 0. |

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Examples

The following example shows how to see the mesh configurations:

```
Device# wireless mesh config
```

show wireless mesh rrm dca status

To display the status of the last DCA run per radio, use the **show wireless mesh rrm dca status** command.

show wireless mesh rrm dca status

| | | |
|---------------------------|--|------------------------------|
| Syntax Description | This command has no keywords or arguments. | |
| Command Default | None | |
| Command Modes | Privileged EXEC(#) | |
| Command History | Release | Modification |
| | Cisco IOS XE Cupertino 17.9.1 | This command was introduced. |

Example

This example shows how to display the status of the last DCA run per radio:

```
Device# show wireless mesh rrm dca status
```

show wireless mesh neighbor

To see the neighbors of all connected mesh APs, use the **show wireless mesh neighbor** command.

show wireless mesh neighbor [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

Syntax Description

| | |
|-----------------------|--|
| neighbor | Shows the neighbors of all connected mesh APs. |
| <i>chassis-number</i> | Enter the chassis number as either 1 or 2. |
| active R0 | Active instance of the active AP filters in Route-processor slot 0. |
| standby R0 | Standby instance of the active AP filters in Route-processor slot 0. |

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

Definition of the field State is as follows:

- **UPDATED**: Adjacency is reachable: communication is symmetric, we can exchange frames with that AP.
- **NEIGH**: Adjacency is parent capable. Local criterion: reachability, strict BGN config, valid cost, potential loops, and so on.
- **CHILD**: Adjacency is actually a child mesh AP (associated to the considered AP).
- **PARENT**: Adjacency is actually the parent mesh AP.
- **DEFAULT**: Adjacency BGN is different than our backhaul configured one.
- **BLOCK**: Adjacency is currently blocklisted due to: auth failures, capwap teardown, and so on.

Examples

The following example shows how to see the neighbors of all connected mesh APs:

```
Device# show wireless mesh neighbor
```

```
AP Name/Radio           Channel  Rate    Link-snr  Flags  State
-----
AP Name : Mesh-AP01
54:9f:c6:fa:5c:71      149     auto    0         40
```


| | | | | | |
|-------------------|-----|------|----|------|----------------------|
| b0:c5:3c:e5:d9:71 | 149 | auto | 22 | 49 | UPDATED NEIGH |
| e8:eb:34:d5:88:d1 | 149 | auto | 0 | 40 | |
| e8:eb:34:d5:8d:d1 | 149 | auto | 18 | 49 | UPDATED CHILD |
| e8:eb:34:d5:94:d1 | 149 | auto | 37 | 4b | UPDATED NEIGH PARENT |
| e8:eb:34:d5:d3:11 | 149 | auto | 31 | 49 | UPDATED NEIGH |
| e8:eb:34:d5:d8:91 | 149 | auto | 0 | 41 | UPDATED |
| e8:eb:34:d5:da:31 | 149 | auto | 18 | 49 | UPDATED NEIGH |
| e8:eb:34:d5:da:51 | 149 | auto | 0 | 1040 | DEFAULT |
| e8:eb:34:d5:dc:d1 | 149 | auto | 9 | 49 | UPDATED NEIGH |
| e8:eb:34:d5:ef:51 | 149 | auto | 0 | 40 | |
| e8:eb:34:d5:f6:51 | 149 | auto | 9 | 49 | UPDATED NEIGH |
| e8:eb:34:d5:fd:51 | 149 | auto | 21 | 49 | UPDATED NEIGH |
| ec:ce:13:9a:89:91 | 149 | auto | 19 | 49 | UPDATED NEIGH |
| ec:ce:13:d7:6f:91 | 149 | auto | 18 | 49 | UPDATED NEIGH |
| ec:ce:13:d7:75:71 | 149 | auto | 19 | 49 | UPDATED NEIGH |
| ec:ce:13:d7:87:91 | 149 | auto | 0 | 41 | UPDATED |
| ec:ce:13:d7:8e:51 | 149 | auto | 6 | 49 | UPDATED NEIGH |

show wireless profile ap priming summary

To view the summary of priming APs, the **show wireless profile ap priming summary** command.

show wireless profile ap priming summary

| | |
|---------------------------|---|
| Syntax Description | The command has no keywords or arguments. |
|---------------------------|---|

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

| | |
|----------------------|-----------------|
| Command Modes | Privileged EXEC |
|----------------------|-----------------|

| Command History | Release | Modification |
|------------------------|-------------------------------|------------------------------|
| | Cisco IOS XE Cupertino 17.9.1 | This command was introduced. |

Example

The following example shows how to view the summary of priming APs:

```
Device# show wireless profile ap priming summary
```

show wireless mobility

To view the wireless mobility summary, use the **show wireless mobility** command.

show wireless mobility { **agent** *mobility-agent-ip* **client summary** | **ap-list ip-address** *ip-address* | **controller client summary** | **dtls connections** | **statistics summary** }

| Syntax Description | |
|---|--|
| agent <i>mobility-agent-ip</i> client summary | Shows the active clients on a mobility agent. |
| ap-list ip-address <i>ip-address</i> | Shows the list of Cisco APs known to the mobility group. |
| controller client summary | Shows the active clients in the subdomain. |
| dtls connections | Shows the DTLS server status. |
| statistics | Shows the statistics for the Mobility manager. |
| summary | Shows the summary of the mobility manager. |

Command Default None

Command Modes Global Configuration

| Command History | Release | Modification |
|-----------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to display a summary of the mobility manager:

```
Device (config)# show wireless mobility ap-list
```

| AP name | AP radio MAC | Controller IP | Learnt from |
|-------------|----------------|---------------|-------------|
| TSIM_AP-101 | 0000.2000.6600 | 9.9.9.2 | Self |
| TSIM_AP-102 | 0000.2000.6700 | 9.9.9.2 | Self |
| TSIM_AP-103 | 0000.2000.6800 | 9.9.9.2 | Self |
| TSIM_AP-400 | 0000.2001.9100 | 9.9.9.2 | Self |
| TSIM_AP-402 | 0000.2001.9300 | 9.9.9.2 | Self |
| TSIM_AP-403 | 0000.2001.9400 | 9.9.9.2 | Self |
| TSIM_AP-406 | 0000.2001.9700 | 9.9.9.2 | Self |
| TSIM_AP-407 | 0000.2001.9800 | 9.9.9.2 | Self |
| TSIM_AP-409 | 0000.2001.9a00 | 9.9.9.2 | Self |

show wireless mobility peer ip

To see the details of the mobility peer using its IP address, use the **show wireless mobility peer ip** command.

show wireless mobility peer ip *ip-address*

| | |
|---------------------------|--|
| Syntax Description | <i>ip-address</i> Mobility peer IPv4 IP address. |
|---------------------------|--|

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

| | |
|----------------------|-----------------|
| Command Modes | Privileged EXEC |
|----------------------|-----------------|

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

Examples

The following example shows how to see the details of the wireless mobility peer using its IP address:

```
Device# show wireless mobility peer ip 209.165.200.224
```

show wireless multicast group summary

To see the wireless multicast group summary, use the **show wireless multicast group summary** command.

show wireless multicast group summary

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Examples

The following example shows how to see the summary of the wireless multicast group:

```
Device# show wireless multicast group summary
```

show wireless mobility summary

To see the wireless mobility manager summary, use the **show wireless mobility summary** command.

show wireless mobility summary

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Examples

The following example shows how to see the wireless mobility manager's summary:

```
Device# show wireless mobility summary
```

show wireless multicast

To display wireless multicast information, use the **show wireless multicast** command in privileged EXEC mode.

show wireless multicast [**source** *source-ip* **group** *group-ip* **vlan** *vlan-id* | **group** *group-ip* **vlan** *vlan-id*]

| Syntax Description | source <i>source-ip</i> (Optional) Specifies the source IPv4 and IPv6 address of multicast traffic. | | | | |
|--------------------------------|--|---------|--------------|--------------------------------|------------------------------|
| Command Default | None | | | | |
| Command Modes | Privileged EXEC | | | | |
| Command History | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.10.1</td> <td>This command was introduced.</td> </tr> </tbody> </table> | Release | Modification | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. | | | | |
| Usage Guidelines | None | | | | |

This example shows how to display the wireless multicast information:

```
Device# show wireless multicast

Multicast                               : Enabled
AP Capwap Multicast                     : Unicast
Wireless Broadcast                       : Disabled
Wireless Multicast non-ip-mcast         : Disabled

Vlan      Non-ip-mcast      Broadcast      MGID
-----
1          Enabled         Enabled        Enabled
2          Enabled         Enabled        Disabled
94         Enabled         Enabled        Disabled

Device# show wireless multicast
Multicast                               : Disabled
AP Capwap Multicast                     : Unicast
Wireless Broadcast                       : Disabled
Wireless Multicast non-ip-mcast         : Disabled
Wireless Multicast link-local           : Enabled
```

show wireless multicast group

To display the information of the wireless-multicast non-ip VLANs or the group, use the **show wireless multicast group** command in privileged EXEC mode.

```
show wireless multicast group {summary | group-ip vlan vlan-id}
```

| Syntax Description | |
|----------------------------|---|
| summary | Displays wireless-multicast non-ip group summary. |
| <i>group-ip</i> | Specifies the group IP address. |
| vlan <i>vlan-id</i> | Specifies the destination group IPv4/IPv6 Address of multicast traffic. |

Command Default None.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

Usage Guidelines None.

Examples

This example shows how to display the wireless-multicast non-ip group summary.

```
Device# show wireless multicast group summary
```


show wireless mesh ethernet daisy-chain summary

To verify the ethernet daisy chain summary, use the **show wireless mesh ethernet daisy-chain summary** command.

show wireless mesh ethernet daisy-chain summary

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged EXEC

Command History

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

The following example shows how to verify the ethernet daisy chain summary:

Device# **show wireless mesh ethernet daisy-chain summary**

| AP Name | BVI | MAC | BGN | Backhaul | Ethernet | STP | Red | |
|---------|----------------|-----|-----------|----------|----------|-----|-----|---------|
| RAP4 | 683b.78bf.15f0 | IOT | Ethernet0 | Up | Up | Dn | Dn | Enabled |
| RAP3 | 683b.78bf.1634 | IOT | Ethernet0 | Up | Up | Dn | Dn | Enabled |
| RAP1 | 6c8b.d383.b4d4 | IOT | Ethernet0 | Up | Up | Dn | Dn | Enabled |
| RAP2 | 6c8b.d383.b4e8 | IOT | Ethernet0 | Up | Up | Up | Dn | Enabled |

show wireless mesh ethernet daisy-chain bgn

To verify the ethernet daisy chain Bridge Group Name (BGN) details, use the **show wireless mesh ethernet daisy-chain bgn** command.

show wireless mesh ethernet daisy-chain bgn *bridge-group-name*

| | |
|---------------------------|---|
| Syntax Description | <i>bridge-group-name</i> Enter the bridge group name. |
|---------------------------|---|

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

| | |
|----------------------|-----------------|
| Command Modes | Privileged EXEC |
|----------------------|-----------------|

| Command History | Release | Modification |
|------------------------|-------------------------------|------------------------------|
| | Cisco IOS XE Bengaluru 17.4.1 | This command was introduced. |

The following example shows how to verify the ethernet daisy chain Bridge Group Name (BGN) details:

Device# **show wireless mesh ethernet daisy-chain bgn <IOT>**

| AP Name | BVI MAC | BGN | Backhaul | Ethernet | STP Red |
|---------|----------------|-----|-----------|-------------|---------|
| RAP4 | 683b.78bf.15f0 | IOT | Ethernet0 | Up Up Dn Dn | Enabled |
| RAP3 | 683b.78bf.1634 | IOT | Ethernet0 | Up Up Dn Dn | Enabled |
| RAP1 | 6c8b.d383.b4d4 | IOT | Ethernet0 | Up Up Dn Dn | Enabled |
| RAP2 | 6c8b.d383.b4e8 | IOT | Ethernet0 | Up Up Up Dn | Enabled |

show wireless performance

To display aggressive load balancing configuration, use the **show wireless performance** command in privileged EXEC mode.

show wireless performance {ap | client} summary

| | | |
|---------------------------|--------------------------------|---|
| Syntax Description | ap summary | Displays aggressive load balancing configuration of access points configured to the controller. |
| | client summary | Displays aggressive load balancing configuration details of the clients. |
| Command Default | No default behavior or values. | |
| Command Modes | Privileged EXEC | |
| Command History | Release | Modification |
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

The following is sample output from the **show wireless performance ap summary** command.

```
Device# show wireless performance ap summary
Number of APs:
```

The following is sample output from the **show wireless performance client summary** command.

```
Device# show wireless performance client summary
Number of Clients:
```

```
MAC Address          AP Name              Status              WLAN/Guest-Lan Auth Protocol Port Wired
-----
```

show wireless pmk-cache

To display information about the pairwise master key (PMK) cache, use the **show wireless pmk-cache** command in privileged EXEC mode.

show wireless pmk-cache[*mac-address mac-addr*]

| | |
|---------------------------|---|
| Syntax Description | mac-address mac-addr (Optional) Information about a single entry in the PMK cache. |
|---------------------------|---|

| | |
|------------------------|--------------------------------|
| Command Default | No default behavior or values. |
|------------------------|--------------------------------|

| | |
|----------------------|-----------------|
| Command Modes | Privileged EXEC |
|----------------------|-----------------|

| Command History | Release | Modification |
|------------------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

The following is sample output from the **show wireless pmk-cache mac-address** command:

```
Device# show wireless pmk-cache mac-address H.H.H
Number of PMK caches in total : 0
```

show wireless probe

To display the advanced probe request filtering configuration and the number of probes sent to the WLAN controller per access point per client and the probe interval in milliseconds, use the **show wireless probe** command in privileged EXEC mode.

show wireless probe

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

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

The following is sample output from the **show wireless probe** command:

```
Device# show wireless probe
Probe request filtering           : Enabled
Number of probes per client per radio fwd from AP: 2
Probe request rate-limiting interval : 500 msec
Aggregate probe request interval  : 500 msec
```

show wireless profile ap priming all

To display the details of priming profiles, use the **show wireless profile ap priming all** command.

show wireless profile ap priming all

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Privileged EXEC (#)

Command History

| Release | Modification |
|-------------------------------|------------------------------|
| Cisco IOS XE Cupertino 17.9.2 | This command was introduced. |

Examples

The following example shows how to display the details of priming profiles:

```
Device# show wireless profile ap priming all
```

| Profile Name | Primary Controller Name | Primary Controller IP | Secondary Controller Name | Secondary Controller IP | Tertiary Controller Name | Tertiary Controller IP | Override |
|--------------|-------------------------|-----------------------|---------------------------|-------------------------|--------------------------|------------------------|----------|
| AP-PRIMING-1 | BGL18-wlc | 209.165.201.1 | BGL17-wlc | 0.0.0.0 | | | Disabled |
| AP-PRIMING-2 | BGL18-wlc | 209.165.201.2 | BGL17-wlc | 209.165.201.3 | BGL12-wlc | | Disabled |

show wireless profile ap priming all

To display the details of priming profiles, use the **show wireless profile ap priming all** command.

show wireless profile ap priming all

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Privileged EXEC (#)

| Command History | Release | Modification |
|-----------------|-------------------------------|------------------------------|
| | Cisco IOS XE Cupertino 17.9.2 | This command was introduced. |

Examples

The following example shows how to display the details of priming profiles:

```
Device# show wireless profile ap priming all
```

| Profile Name | Primary Controller Name | Primary Controller IP | Secondary Controller Name | Secondary Controller IP | Tertiary Controller Name | Tertiary Controller IP | Override |
|--------------|-------------------------|-----------------------|---------------------------|-------------------------|--------------------------|------------------------|----------|
| AP-PRIMING-1 | BGL18-wlc | 209.165.201.1 | BGL17-wlc | 209.165.201.2 | | 0.0.0.0 | Disabled |
| AP-PRIMING-2 | BGL18-wlc | 209.165.201.2 | BGL17-wlc | 209.165.201.2 | BGL12-wlc | 209.165.201.3 | Disabled |

show wireless profile airtime-fairness mapping

To view the ATF policy mapping with the wireless profiles, use the **show wireless profile airtime-fairness mapping** command.

show wireless profile airtime-fairness mapping

| | |
|---------------------------|--------------------------------|
| Syntax Description | This command has no arguments. |
|---------------------------|--------------------------------|

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

| | |
|----------------------|----------------------|
| Command Modes | Global configuration |
|----------------------|----------------------|

| | | |
|------------------------|--------------------------------|------------------------------|
| Command History | Release | Modification |
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the ATF policy mapping with the wireless profiles:

```
Device# show wireless profile airtime-fairness mapping
Policy Profile           Band      ATF Policy           Weight
Client Sharing  Availability
-----
WGB                No                2.4GHz                -        -
WGB                No                5GHz                  -        -
Policy1            No                2.4GHz                -        -
Policy1            No                5GHz                  -        -
Test WBG           No                2.4GHz                -        -
Test WBG           No                5GHz                  -        -
profile-name      No                2.4GHz                -        -
Enabled           Yes                atf-policy-name      5
```


show wireless profile airtime-fairness summary

To view the summary of air time fairness profiles, use the **show wireless profile airtime-fairness summary** command.

show wireless profile airtime-fairness summary

Syntax Description This command has no arguments.

Command Default None

Command Modes Global configuration

| Command History | Release | Modification |
|-----------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the summary of air time fairness profiles:

```
Device# show wireless profile airtime-fairness summary
Policy Id      Policy Name      Weight      Client Sharing
-----
1              atf-policy-name  5           Enabled
```

show wireless profile ap packet-capture

To view the AP packet capture information, use the **show wireless profile ap packet-capture** command.

show wireless profile ap packet-capture { *detailed profile-name* | **summary** }

| | |
|---------------------------|--|
| Syntax Description | <i>profile-name</i> AP packet capture profile. |
|---------------------------|--|

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

| | |
|----------------------|-----------------|
| Command Modes | Privileged EXEC |
|----------------------|-----------------|

| Command History | Release | Modification |
|------------------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

Usage Guidelines

Example

The following example shows how to view the AP packet capture information:

```
Device# show wireless profile ap packet-capture summary
Number of AP packet capture profiles: 3
```

| Profile Name | Buffer | Duration(M | Packet Len | FTP IP |
|--------------|--------|------------|------------|-----------|
| test | 1200 | 20 | 0 | 9.1.0.101 |
| test1 | 2048 | 10 | 0 | 0.0.0.0 |
| tets1 | 1024 | 10 | 0 | 0.0.0.0 |

Example

The following example shows how to view the detailed AP packet capture information of an AP profile:

```
Device# show wireless profile ap packet-capture detailed test1
```

```
Profile Name : test1
Description :
-----
Buffer Size      : 2048 KB
Capture Duration : 10 Minutes
Truncate Length  : packet length
FTP Server IP    : 0.0.0.0
FTP path         :
FTP Username     :

Packet Classifiers
 802.11 Control  : Enabled
 802.11 Mgmt     : Enabled
 802.11 Data     : Disabled
Dot1x           : Disabled
```

```
ARP           : Disabled
IAPP          : Disabled
IP            : Disabled
TCP           : Disabled
TCP port     : all
UDP           : Disabled
UDP port     : all
Broadcast    : Disabled
Multicast    : Disabled
```

show wireless profile calendar-profile detailed

To view the calendar profile details for a specific profile name, use the **show wireless profile calendar-profile detailed** command.

show wireless profile calendar-profile detailed *profile-name*

| | |
|---------------------------|--|
| Syntax Description | <i>profile-name</i> Specifies the calendar profile name. |
|---------------------------|--|

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

| | |
|----------------------|-----------------|
| Command Modes | Privileged EXEC |
|----------------------|-----------------|

| Command History | Release | Modification |
|------------------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.12.1 | This command was introduced. |

This example shows how to view the calendar profile details for a specific profile name:

```
Device# show wireless profile calendar-profile detailed daily_calendar_profile
Calendar profiles : daily_calendar_profile
-----
Recurrence : DAILY
Start Time : 09:00:00
End Time : 17:00:00
```

show wireless profile calendar-profile summary

To view the summary of calendar profiles, use the **show wireless profile calendar-profile summary** command.

show wireless profile calendar-profile summary

| | | |
|---------------------------|--|------------------------------|
| Syntax Description | This command has no keywords or arguments. | |
| Command Default | None | |
| Command Modes | Privileged EXEC | |
| Command History | Release | Modification |
| | Cisco IOS XE Gibraltar 16.12.1 | This command was introduced. |

This example shows the summary of calendar profiles:

```
Device# show wireless profile calendar-profile summary
Number of Calendar Profiles: 3
Profile-Name
-----
monthly_25_profile
weekly_mon_profile
daily_calendar_profile
```

show wireless profile fabric detailed

To view the details of a given fabric profile name, use the **show wireless profile fabric detailed** command.

show wireless profile fabric detailed *fabric_profile_name*

| | | |
|---------------------------|--------------------------------|------------------------------|
| Syntax Description | This command has no arguments. | |
| Command Default | None | |
| Command Modes | Global configuration | |
| Command History | Release | Modification |
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the details of a given fabric profile name:

```
Device# show wireless profile fabric detailed test1
Profile-name      : test-fabric
VNID              : 12
SGT               : 5
```

show wireless profile flex

To see the flex parameters of an wireless profile, use the **show wireless profile flex** command.

```
show wireless profile flex { detailed flex-profile-name chassis {chassis-number | active | standby } R0
} | summary chassis {chassis-number | active | standby} R0}
```

| Syntax Description | | |
|-----------------------|--|--|
| detailed | Shows the flex-profile detailed parameters | |
| summary | Show the flex-profile summary. | |
| <i>chassis-number</i> | Chassis number. Valid range is 1–2. | |
| active | Active instance. | |
| standby | Standby instance. | |
| R0 | Route-Processor slot 0. | |

Command Default None

Command Modes Privileged EXEC

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

Examples

The following example shows how to see the flex parameter's summary of the wireless profile:

```
Device# show wireless profile flex summary
```

show wireless profile policy all

To display detailed output of all policy profiles, use the **show wireless profile policy all** command.

show wireless profile policy all

| | | |
|---------------------------|--|---|
| Syntax Description | This command has no keywords or arguments. | |
| Command Default | None | |
| Command Modes | Privilege EXEC (#) | |
| Command History | Release | Modification |
| | Cisco IOS XE Gibraltar 16.12.1 | This command was introduced. |
| | Cisco IOS XE Amsterdam 17.3.5 | The output of the command was modified to include ARP activity information. |

Example

This example shows how to view the detailed output of all policy profiles:

```
Device# show wireless profile policy all

Policy Profile Name      : policy_name
Description              :
Status                  : ENABLED
.
.
.
!the section of the output that shows whether ARP is enabled or disabled in the policy
profile.
ARP Activity Limit
  Exclusion               : ENABLED
  PPS                   : 100
  Burst Interval        : 5
```


show wireless profile policy detailed

To display the wireless policy profile details, use the **show wireless profile policy detailed** command.

show wireless profile policy detailed *policy-profile-name*

| Syntax Description | This command has no keywords or arguments. | | | | |
|-------------------------------|---|---------|--------------|-------------------------------|------------------------------|
| Command Default | None | | | | |
| Command Modes | Privilege EXEC (#) | | | | |
| Command History | <table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>Cisco IOS XE Amsterdam 17.2.1</td><td>This command was introduced.</td></tr></tbody></table> | Release | Modification | Cisco IOS XE Amsterdam 17.2.1 | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE Amsterdam 17.2.1 | This command was introduced. | | | | |

Example

This example displays the wireless policy profile details:

```
Device#show wireless profile policy detailed policy-profile-name
```

show wireless profile mesh detailed

To verify the mesh profile, use the **show wireless profile mesh detailed** command.

show wireless profile mesh detailed *profile-name*

| Syntax Description | <i>profile-name</i> Enter the profile name. | | | | |
|-------------------------------|---|---------|--------------|-------------------------------|------------------------------|
| Command Default | None | | | | |
| Command Modes | Privileged EXEC | | | | |
| Command History | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Bengaluru 17.4.1</td> <td>This command was introduced.</td> </tr> </tbody> </table> | Release | Modification | Cisco IOS XE Bengaluru 17.4.1 | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE Bengaluru 17.4.1 | This command was introduced. | | | | |

The following example shows how to verify the mesh profile:

```
Device# show wireless profile mesh detailed default-mesh-profile

Mesh Profile Name : default-mesh-profile
-----
Description : default mesh profile
Bridge Group Name : IOT
Strict match BGN : ENABLED
Amsdu : ENABLED
Background Scan : ENABLED
Channel Change Notification : ENABLED
Backhaul client access : ENABLED
Ethernet Bridging : ENABLED
Ethernet Vlan Transparent : DISABLED
Daisy Chain STP Redundancy : ENABLED
Full Sector DFS : ENABLED
IDS : ENABLED
Multicast Mode : In-Out
Range in feet : 12000
Security Mode : EAP
Convergence Method : Standard
LSC only Authentication : DISABLED
Battery State : ENABLED
Authorization Method : eap_methods
Authentication Method : eap_methods
Backhaul tx rate(802.11bg) : auto
Backhaul tx rate(802.11a) : auto
```

show wireless profile radio summary

To display the wireless radio profile summary, use the **show wireless profile radio summary** command.

show wireless profile radio summary

| Syntax Description | This command has no keywords or arguments. | | | | |
|-------------------------------|---|---------|--------------|-------------------------------|------------------------------|
| Command Default | None | | | | |
| Command Modes | Privileged EXEC mode | | | | |
| Command History | <table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>Cisco IOS XE Bengaluru 17.6.1</td><td>This command was introduced.</td></tr></tbody></table> | Release | Modification | Cisco IOS XE Bengaluru 17.6.1 | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE Bengaluru 17.6.1 | This command was introduced. | | | | |
| Usage Guidelines | None | | | | |

Example

The following example shows you how to display the wireless radio profile summary:

```
Device# show wireless profile radio summary
```

show wireless profile tunnel summary

To display the wireless tunnel-profile summary, use the **show wireless profile tunnel summary** command.

show wireless profile tunnel summary

| | | |
|---------------------------|--|------------------------------|
| Syntax Description | This command has no keywords or arguments. | |
| Command Default | None | |
| Command Modes | Privileged EXEC (#) | |
| Command History | Release | Modification |
| | Cisco IOS XE Gibraltar 16.11.1 | This command was introduced. |

Example

This example shows how to display the wireless tunnel profile summary:

```
Device# show wireless profile tunnel summary
```

```
Profile Name          AAA-Override AAA-Proxy DHCP Opt82 Enabled
-----
eogre_tunnel          No           No       Yes   Yes
eogre_tunnel_set      No           No       Yes   No
eogre_tunnel_snmp     No           No       No    No
```

show wireless redundancy statistics

To see the high availability statistics, use the **show wireless redundancy statistics** command.

```
show wireless redundancy statistics {ap-group | wncdallchassis {chassis-num | active | standby} R0}
{ap-recovery | {instance-id | all | chassis {chassis-num | active | standby} R0}}
{client-group | wncdallchassis {chassis-num | active | standby} R0}
{client-recovery | {mobilityd | sisf} chassis {chassis-num | active | standby} R0}
{wncd | {instance-id | all | chassis {chassis-num | active | standby} R0}}
```

Syntax Description

chassis-number Enter the chassis number as either 1 or 2.

active R0 Active instance of the configuration in Route-processor slot 0.

standby R0 Standby instance of the configuration in Route-processor slot 0.

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Examples

The following example shows how to see all the statistics for WNCD :

show wireless rfid

To display RFID tag information, use the **show wireless rfid** command in privileged EXEC mode.

show wireless rfid { **client** | **detail** *rfid-mac-address* | **stats** | **summary** }

| Syntax Description | | |
|-------------------------|--|---|
| client | | Displays the summary of RFID tags that are clients. |
| detail | | Displays information about a particular RFID tag. |
| stats | | Displays RFID statistics. |
| summary | | Displays summary information for all known RFID tags. |
| <i>rfid-mac-address</i> | | RFID MAC address. |

Command Default None

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

Example

This example shows how to view RFID information:

```
Device# show wireless rfid summary
```

```
Total RFID entries: : 16
Total Unique RFID entries : 16
RFID ID VENDOR Closet AP RSSI Time Since Last Heard
0012.b80a.c791 Cisco 7069.5a63.0520 -31 1 minute 40 seconds ago
0012.b80a.c953 Cisco 7069.5a63.0460 -33 2 minutes 15 seconds ago
0012.b80b.806c Cisco 7069.5a63.0260 -45 22 seconds ago
0012.b80d.e9f9 Cisco 7069.5a63.0460 -38 2 minutes 37 seconds ago
0012.b80d.ea03 Cisco 7069.5a63.0520 -43 2 minutes 38 seconds ago
0012.b80d.ea6b Cisco 7069.5a63.0460 -39 2 minutes 35 seconds ago
0012.b80d.ebe8 Cisco 7069.5a63.0520 -43 1 minute 31 seconds ago
0012.b80d.ebeb Cisco 7069.5a63.0520 -43 2 minutes 37 seconds ago
0012.b80d.ec48 Cisco 7069.5a63.0460 -42 2 minutes 16 seconds ago
0012.b80d.ec55 Cisco 7069.5a63.0520 -41 1 second ago
```

show wireless stats ap name

To display the wireless AP BSSID statistics, use the **show wireless stats ap name** *ap-name* **dot11 24ghz slot 0** *wlan-name 1-4096* **statistics**

show wireless stats ap name *ap-name* **dot11 24ghz slot 0** *wlan-name 1-4096* **statistics**

| | | |
|---------------------------|-------------------------------|--|
| Syntax Description | <i>ap-name</i> | Specifies the name of the AP. |
| | <i>wlan-name</i> | Specifies the name of the WLAN. |
| | <i>wlan-id</i> | Specifies the WLAN ID. The value range is 1 to 4096. |
| Command Default | None | |
| Command Modes | Privileged EXEC (#) | |
| Command History | Release | Modification |
| | Cisco IOS XE Amsterdam 17.2.1 | This command was introduced. |

Example

This example show how to display the wireless AP BSSID statistics:

```
Device#show wireless stats ap name ap-name dot11 24ghz slot 0 wlan-name 1-4096 statistics
BSSID           : 7069.5a38.112e
WLAN ID         : 18
Client Count    : 1
TX Statistics
-----
Mgmt           Retries      Data Bytes      Data Retries      Subframe Retries
-----
12             18             16081           18                 0
RX Statistics
-----
Mgmt           Data Bytes
-----
74             17693
Data Distribution
-----
Bytes           RX           TX
-----
0-64            55           93
65-128          66           40
129-256         21           5
257-512         10           3
513-1024        1            9
1025-2048       0            1
2049-4096       0            0
4097-8192       0            0
8193-16384      0            0
16385-32768     0            0
32769-65536     0            0
```

show wireless stats ap name

| | | |
|----------------|---|---|
| 65537-131072 | 0 | 0 |
| 131073-262144 | 0 | 0 |
| 262145-524288 | 0 | 0 |
| 524289-1048576 | 0 | 0 |

WMM Statistics

| | RX | TX |
|-------------|-----|----|
| Voice | 0 | 43 |
| Video | 0 | 0 |
| Best Effort | 154 | 39 |
| Background | 0 | 0 |

MCS

| MCS | RX | TX |
|------|------|----|
| mcs0 | 39 | 0 |
| mcs1 | 2 | 0 |
| mcs2 | 5 | 0 |
| mcs3 | 7 | 0 |
| mcs4 | 25 | 0 |
| mcs5 | 59 | 0 |
| mcs6 | 290 | 0 |
| mcs7 | 1148 | 3 |
| mcs8 | 2288 | 0 |
| mcs9 | 4440 | 2 |

show wireless stats ap image-download

To verify the AP image download statistics, use the **show wireless stats ap image-download** command in privileged EXEC mode..

```
show wireless stats ap image-download [ chassis { chassis_number | active | standby } R0 ]
```

| Syntax Description | Parameter | Description |
|--------------------|-----------------------|--|
| | chassis | Specifies the chassis for AP image download. |
| | <i>chassis_number</i> | Chassis number, which can be either 1 or 2. |
| | active | Specifies an active instance. |
| | standby | Specifies a standby instance. |
| | R0 | Specifies the route processor for Slot 0. |

Command Default None

Command Modes Privileged EXEC (#)

| Command History | Release | Modification |
|-----------------|-----------------------------|------------------------------|
| | Cisco IOS XE Dublin 17.11.1 | This command was introduced. |

Examples

The following example shows how to verify the AP image download statistics:

```
Device# show wireless stats ap image-download

AP image download info for last attempt
AP Name Count ImageSize StartTime EndTime Diff(secs) Predownload
Aborted Method
-----
JK3800 1 59228160 09/06/21 15:20:53 09/06/21 15:21:36 43 No
No HTTPS
mysore1 4 40509440 08/30/21 22:51:08 08/30/21 22:51:51 44 No
No HTTPS
```

show wireless stats client delete reasons

To verify total client delete reasons, use the **show wireless stats client delete reasons** command.

show wireless stats client delete reasons

| | | |
|---------------------------|--|------------------------------|
| Syntax Description | This command has no keywords or arguments. | |
| Command Default | None | |
| Command Modes | Privileged EXEC(#) | |
| Command History | Release | Modification |
| | Cisco IOS XE Amsterdam 17.1.1 | This command was introduced. |

This example shows how to verify the total client delete reasons:

```
Device# show wireless stats client delete reasons

Total client delete reasons
-----
Controller deletes
-----
-----
No Operation                               : 0
Unknown                                    : 0
Session Manager                            : 0
Connection timeout                         : 0
Datapath plumb                             : 0
WPA key exchange timeout                   : 0
802.11w MAX SA queries reached              : 0
Client deleted during HA recovery           : 0
Inter instance roam failure                : 0
Inter instance roam success                : 0
Inter controller roam success              : 0
Due to mobility failure                    : 0
NAS error                                   : 0
Policy Manager internal error               : 0
80211v smart roam failed                   : 0
DOT11v association failed                  : 0
DOT11r pre-authentication failure          : 0
SAE authentication failure                 : 0
DOT11 failure                              : 0
DOT11 SAE invalid message                  : 0
DOT11 denied data rates                    : 0
802.11v Client RSSI lower than the association RSSI threshold : 0
invalid QoS parameter                      : 0
DOT11 IE validation failed                 : 0
DOT11 group cipher in IE validation failed : 0
DOT11 invalid pairwise cipher              : 0
DOT11 invalid AKM                          : 0
DOT11 unsupported RSN version              : 0
DOT11 invalid RSNIE capabilities           : 0
DOT11 received invalid PMKID in the received RSN IE : 0
```

```

DOT11 received invalid PMK length           : 0
DOT11 invalid MDIE                         : 0
DOT11 invalid FT IE                       : 0
DOT11 AID allocation conflicts             : 0
AVC client re-anchored at the foreign controller : 0
Client EAP ID timeout                      : 0
Client DOT1x timeout                      : 0
Malformed EAP key frame                   : 0
EAP key install bit is not expected       : 0
EAP key error bit is not expected        : 0
EAP key ACK bit is not expected          : 0
Invalid key type                          : 0
EAP key secure bit is not expected       : 0
key description version mismatch         : 0
wrong replay counter                      : 0
EAP key MIC bit expected                  : 0
MIC validation failed                    : 0
MAC theft                                 : 0
IP theft                                  : 0
Policy bind failure                      : 0
Web authentication failure                : 0
802.1X authentication credential failure : 0
802.1X authentication timeout            : 0
802.11 authentication failure            : 0
802.11 association failure                : 0
Manually excluded                        : 0
DB error                                  : 0
Anchor creation failure                  : 0
Anchor invalid Mobility BSSID             : 0
Anchor no memory                         : 0
Call admission controller at anchor node : 0
Supplicant restart                       : 0
Port admin disabled                      : 0
Reauthentication failure                  : 0
Client connection lost                   : 0
Error while PTK computation               : 0
MAC and IP theft                         : 0
QoS policy failure                       : 0
QoS policy send to AP failure            : 0
QoS policy bind on AP failure            : 0
QoS policy unbind on AP failure          : 0
Static IP anchor discovery failure        : 0
VLAN failure                             : 0
ACL failure                              : 0
Redirect ACL failure                     : 0
Accounting failure                       : 0
Security group tag failure               : 0
FQDN filter definition does not exist     : 0
Wrong filter type, expected postauth FQDN filter : 0
Wrong filter type, expected preauth FQDN filter : 0
Invalid group id for FQDN filter valid range 1..16 : 0
Policy parameter mismatch                : 0
Reauth failure                           : 0
Wrong PSK                                 : 0
Policy failure                            : 0
AAA server unavailable                   : 0
AAA server not ready                     : 0
No dot1x method configuration            : 0
Association connection timeout           : 0
MAC-AUTH connection timeout              : 0
L2-AUTH connection timeout               : 0
L3-AUTH connection timeout               : 0
Mobility connection timeout              : 0
static IP connection timeout              : 0

```

show wireless stats client delete reasons

```

SM session creation timeout           : 0
IP-LEARN connection timeout          : 0
NACK IFID exists                     : 0
Guest-LAN invalid MBSSID             : 0
Guest-LAN no memory                  : 0
Guest-LAN ceate request failed       : 0
EoGRE Reset                          : 0
EoGRE Generic Join Failure           : 0
EoGRE HA-Reconciliation              : 0
Wired idle timeout                   : 0
IP Update timeout                    : 0
SAE Commit received in Associated State : 0
NACK IFID mismatch                   : 0
EoGRE Invalid VLAN                  : 0
EoGRE Empty Domain                  : 0
EoGRE Invalid Domain                 : 0
EoGRE Domain Shut                   : 0
EoGRE Invalid Gateway               : 0
EoGRE All Gateways down              : 0
EoGRE Flex - no active gateway       : 0
EoGRE Rule Matching error            : 0
EoGRE AAA Override error             : 0
EoGRE client onboarding error        : 0
EoGRE Mobility Handoff error         : 0
L3 VLAN Override connection timeout  : 0
Delete received from AP              : 0
QoS failure                          : 0
WPA group key update timeout         : 0
DOT11 unsupported client capabilities : 0
DOT11 association denied unspecified : 0
DOT11 AP have insufficient bandwidth : 0
DOT11 invalid QoS parameter          : 0
Client not allowed by assisted roaming : 0
Wired client deleted due to WGB delete : 0
Client Abort                         : 0
Mobility peer delete                 : 0
No IP                                : 0
BSSID down                          : 0
DOT11 QoS policy                     : 0
Roam across policy profile deny      : 0
4WAY handshake failure - M1 issue    : 0
4WAY handshake failure - M3 issue    : 0
Exclusion policy template fail       : 0
DOT11 Cipher Suite Rejected         : 0
WLAN-ID mismatch in access accept failures : 0
EasyPSK AAA unknown error           : 0
EasyPSK unspecified error            : 0
EasyPSK PSK mismatch error          : 0
EasyPSK radius busy error           : 0
EasyPSK limit reached error         : 0
EasyPSK bad 802.1X frame error      : 0
EasyPSK missing parameter error     : 0
Supplicant name failure              : 0
User name failure                    : 0
Service set ID failure               : 0
Anchor VLAN ID failure               : 0
PSK failure                          : 0
PSK mode failure                     : 0
Interim interval failure             : 0
Link-local bridging VLAN failure     : 0
Link-local bridging VLAN failure     : 0
Maximum client limit reached on AP   : 0
Maximum client limit reached on AP per wlan : 0
Maximum client limit reached on AP radio per wlan : 0

```

```

Maximum client limit reached on AP radio           : 0
L3 Access Roam across policy profile deny         : 0
L3 Access Inter controller roam deny              : 0
-----
Informational Delete Reason
-----
Mobility WLAN down                               : 0
AP upgrade                                       : 0
L3 authentication failure                       : 0
AP down/disjoin                                 : 0
MAC authentication failure                      : 0
Due to SSID change                             : 0
Due to VLAN change                             : 0
Admin deauthentication                         : 0
Session timeout                                : 0
Idle timeout                                   : 0
Supplicant request                             : 0
Mobility tunnel down                           : 0
DOT11v timer timeout                           : 0
DOT11 max STA                                  : 0
IAPP disassociation for wired client           : 0
Wired WGB change                               : 0
Wired VLAN change                             : 0
WGB Wired client joins as a direct wireless client : 0
Incorrect credentials                          : 0
Wired client cleanup due to WGB roaming        : 0
Radio Down                                     : 0
Mobility failure on fast roam                  : 0
Due to IP Zone change                         : 0
Access denied due to Locally Administered MAC Address : 0
-----
Client initiate delete
-----
Deauthentication or disassociation request      : 0
Client DHCP                                    : 0
Client EAP timeout                             : 0
Client 8021x failure                           : 0
Client device idle                             : 0
Client captive portal security failure          : 0
Client decryption failure                      : 0
Client interface disabled                     : 0
Client user triggered disassociation           : 0
Client miscellaneous reason                   : 0
Unknown                                        : 0
Client peer triggered                          : 0
Client beacon loss                             : 0
STA triggered PMK timeout                      : 0
Excess ARP activity                            : 0
Excess NDP activity                            : 0
Unspecified QOS failure                       : 0
Dpath encode failed                           : 0
VRF-VLAN mismatch failures                    : 0
-----
AP Deletes
-----
When client is sending disassociation          : 0
Idle timeout                                   : 0
Client ACL mismatch                           : 0
AP authentication stop                        : 0
Association expired at AP                     : 0
4-way handshake failed                        : 0
DHCP timeout                                  : 0
Reassociation timeout                         : 0

```

show wireless stats client delete reasons

```

SA query timeout : 0
Intra AP roam : 0
Channel switch at AP : 0
Bad AID : 0
AP requests for client deletion : 0
Interface reset : 0
All on slot : 0
Link to client has changed and uplink can be reaper : 0
Slot disable : 0
MIC failure : 0
VLAN delete : 0
Channel change : 0
Stop reassociation : 0
Packet maximum retry : 0
Transmission deauthentication : 0
Sensor station timeout : 0
Age timeout : 0
Transmission threshold fail : 0
Uplink receive timeout : 0
Sensor scan next radio : 0
Sensor scan other BSSID : 0
Authentication timeout and web-auth timeout : 0
Sending deauthentication packet to client : 0
AP IP learn timeout : 0
Flex group change : 0
EAPOL log off : 0
EAP request timeout : 0
4way handshake failure : 0
MIC validation : 0
Wrong replay counter : 0
AP tunnel down : 0
Inter roam : 0
Unknown client : 0
Reauthentication timeout : 0
Continuous idle timeout : 0
RLDP cleanup : 0
Intra-switch roam : 0
PEM cleanup : 0
RLAN Central switch : 0
RLAN data path add failure : 0
RLAN Delete : 0
RLAN Inactive timeout : 0
RLAN MAB failure : 0
CLSM No memory counter : 0
CLSM BSSID mismatch : 0
CLSM No ACL found : 0
CLSM no parent WGB found : 0
CLSM Key plumb failure : 0
CLSM Mesh key plumb failure : 0
CLSM data path add fail : 0
CLSM Authentication response reject : 0
CLSM Authentication response send failure : 0
CLSM Association response send failure : 0
CLSM association response failure with status : 0
CLSM Webauth timer expired : 0
CLSM Dot1x timer expired : 0
CLSM deauthentication and disassociation send failure : 0
Driver event Class3 received : 0
Driver event PsPoll when not authenticated : 0
Driver event ioctl error : 0
Flex FT failure : 0
CLSM driver add failure : 0
Driver client not found : 0
Driver management packet allocation failure : 0

```

```

Driver invalid cipher : 0
Driver invalid association identifier : 0
Driver invalid key : 0
Driver firmware set key failure : 0
Driver found invalid HT VHT rates : 0
Driver found invalid legacy rates : 0
Driver found no overlapping legacy rates : 0
Driver found maximum VHT streams : 0
Driver found association identifier in use : 0
Driver found too many association requests : 0
Driver found cipher attach failure : 0
Driver found algorithm mismatch : 0
Driver found invalid key length : 0
Driver found invalid key index : 0
Driver rejected association due to authentication failure : 0
Driver found client addition to internal records failure : 0
Driver found client association entry failure : 0
Driver found client additions to firmware failure : 0
Driver related internal failure : 0
AP limiting maximum client per AP : 0
AP limiting maximum client per AP radio per wlan : 0
AP limiting maximum client per AP radio : 0

```

PC Analytics stats:

```

-----
Report Type          Processed Reports
-----
PC_STA_INFO          : 0
PC_NEIGH_INFO        : 0
PC_LOW_RSSI          : 0
PC_TEMP_DISCONN     : 0
PC_AP_FAILURE        : 0
PC_UNKNOWN_AP        : 0

```

```

-----
Report Type          Dropped Reports
-----
PC_STA_INFO          : 0
PC_NEIGH_INFO        : 0
PC_LOW_RSSI          : 0
PC_TEMP_DISCONN     : 0
PC_AP_FAILURE        : 0
PC_UNKNOWN_AP        : 0

```

show wireless statistics mobility

To see the wireless mobility manager statistics, use the **show wireless stats mobility** command.

show wireless stats mobility {**dtls** | **messages**} [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

Syntax Description

| | |
|-----------------------|--|
| dtls | View the mobility dtls messages statistics. |
| messages | View the mobility messages statistics. |
| <i>chassis-number</i> | Enter the chassis number as either 1 or 2. |
| active | Active instance of the configuration in Route-processor slot 0. |
| standby | Standby instance of the configuration in Route-processor slot 0. |

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Examples

The following example shows how to see the statistics of the wireless mobility manager:

```
Device# show wireless stats mobility
```


show wireless stats mesh packet error

To see the packet statistics of all connected mesh APs, use the **show wireless stats mesh packet error** command.

```
show wireless stats mesh packet error [ chassis {chassis-number | active | standby} R0]
```

Syntax Description

| | |
|-------------------|--|
| packet | Shows packet statistics information. |
| error | Shows packet statistics of all connected mesh APs. |
| active R0 | Active instance of the active AP filters in Route-processor slot 0. |
| standby R0 | Standby instance of the active AP filters in Route-processor slot 0. |

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Examples

The following example shows how to see the packet error statistics of all connected mesh APs:

```
Device# show wireless stats mesh packet error
```

show wireless stats pmk-propagation

To view the PMK propagation statistics on the Cisco wireless controller, use the **show wireless stats pmk-propagation** command in privileged EXEC mode.

show wireless stats pmk-propagation

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Privileged EXEC (#)

| Command History | Release | Modification |
|-----------------|-------------------------------|------------------------------|
| | Cisco IOS XE Cupertino 17.8.1 | This command was introduced. |

Examples

The following example shows the PMK propagation statistics on the Cisco Wireless controller:

```
Device# show wireless stats pmk-propagation
```

| Site-Tag | Bulk Sync Success | Bulk Sync Failure | Incremental Sync Failure |
|---------------|-------------------|-------------------|--------------------------|
| flex-site-tag | 97 | 0 | 0 |

show wireless stats mesh security and queue

To see the mesh queue and security statistics of all connected mesh APs, use the **show wireless stats mesh** command.

show wireless stats mesh {**security** | **queue**} [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

| Syntax Description | | |
|-----------------------|--|--|
| queue | Shows queue statistics of all connected mesh APs. | |
| security | Shows security statistics of all connected mesh APs. | |
| <i>chassis-number</i> | Enter the chassis number as either 1 or 2. | |
| active R0 | Active instance of the active AP filters in Route-processor slot 0. | |
| standby R0 | Standby instance of the active AP filters in Route-processor slot 0. | |

Command Default None

Command Modes Privileged EXEC

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

Examples

The following example shows how to see the security statistics of all connected mesh APs:

```
Device# show wireless stats mesh security
```

show wireless stats client detail

To verify the statistics about client, use the **show wireless stats client detail** command.

show wireless stats client detail

| | | |
|---------------------------|--|------------------------------|
| Syntax Description | This command has no keywords or arguments. | |
| Command Default | None | |
| Command Modes | Privileged EXEC | |
| Command History | Release | Modification |
| | Cisco IOS XE Amsterdam 17.1.1 | This command was introduced. |

This example shows how to verify the statistics about client:

```
Device# show wireless stats client detail
[...]
Total L3 VLAN Override vlan change received : 1
Total L3 VLAN Override disassociations sent : 1
Total L3 VLAN Override re-associations received : 1
Total L3 VLAN Override successful VLAN change : 1
[...]
L3 VLAN Override connection timeout : 0
```

show wireless stats redundancy config database

To view the high availability redundancy configuration statistics, use the **show wireless stats redundancy config database** command.

```
show wireless stats redundancy config database { mobility | nmspd | rrm | wncd | wncmgrd
} instance-id chassis { chassis-num | active | standby } R0
```

Syntax Description

| | |
|--------------------|---|
| mobility | Specifies the statistics of Mobilityd configuration database. |
| nmspd | Specifies the statistics of NMSPD configuration database. |
| rrm | Specifies the statistics of RRM configuration database. |
| wncd | Specifies the statistics of WNCd configuration database. |
| wncmgrd | Specifies the statistics of WNCd configuration database. |
| <i>instance-id</i> | Instance ID. Valid values range from 0 to 7. |
| chassis | Specifies the chassis. |
| <i>chassis-num</i> | Chassis number. |
| active | Specifies the active instance. |
| standby | Specifies the standby instance. |
| R0 | Specifies the route processor slot. |

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following example shows how to view the high availability redundancy configuration statistics:

```
Device# show wireless stats redundancy config database wncd 0 chassis 1 R0

Wncd Configuration Sync Statistics
  Index   Number of Locks   Duration(sec)   Threshold-count   Max-Duration(nsec)
-----
      1         535             127             1                1112156700
```

show wireless summary

To display the number of access points, radios and wireless clients known to the controller, use the **show wireless summary** command in privileged EXEC mode.

show wireless summary

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

The following is sample output from the **show wireless summary** command:

```
Device# show wireless summary
```

```
Access Point Summary
```

| | Total | Up | Down |
|-------------|-------|----|------|
| 802.11a/n | 2 | 2 | 0 |
| 802.11b/g/n | 2 | 2 | 0 |
| All APs | 2 | 2 | 0 |

```
Client Summary
```

```
Current Clients : 1
Excluded Clients: 0
Disabled Clients: 0
```

show wireless tag rf

To display the details of wireless RF tag, use the **show wireless tag rf** command.

show wireless tag rf { **summary** | **detailed** } *rf-tag-name*

Syntax Description

summary Displays the summary of all RF tags.

detailed Displays details of an RF tag.

rf-tag-name RF tag name.

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Example

The following example shows the sample output of **show wireless tag rf summary** command:

```
Device# show wireless tag rf summary
```

```
Number of RF Tags: 1
```

```
RF tag name           Description
-----
default-rf-tag       default RF tag
```

show wireless urlfilter details

To view the details of a specified wireless URL filter, use the **show wireless urlfilter details** command.

show wireless urlfilter details *list-name*

| | | |
|---------------------------|--------------------------------|------------------------------|
| Syntax Description | This command has no arguments. | |
| Command Default | None | |
| Command Modes | Global configuration | |
| Command History | Release | Modification |
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the details of a specified wireless URL filter:

```
Device# show wireless urlfilter details urllist_flex_preauth
List Name..... : urllist_flex_preauth
Filter ID..... : 1
Filter Type..... : PRE-AUTH
Action..... : PERMIT
Redirect server ipv4..... : 8.8.8.8
Redirect server ipv6..... : 2001:0300:0008:0000:0000:0000:0000:0081
Configured List of URLs
  URL..... : url1.dns.com
```


show wireless urlfilter summary

To view the summary of all wireless URL filters, use the **show wireless urlfilter summary** command.

show wireless urlfilter summary

| | | |
|---------------------------|--------------------------------|------------------------------|
| Syntax Description | This command has no arguments. | |
| Command Default | None | |
| Command Modes | Global configuration | |
| Command History | Release | Modification |
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the summary of all wireless URL filters:

```
Device# show wireless urlfilter summary
Black-list      - DENY
White-list      - PERMIT
Filter-Type     - Specific to Local Mode

URL-List              ID  Filter-Type  Action  Redirect-ipv4  Redirect-ipv6
-----
urllist_flex_preauth  1   PRE-AUTH    PERMIT   8.8.8.8
2001:0300:0008:0000:0000:0000:0000:0081
```

show wireless vlan details

To see the VLAN details, use the **show wireless vlan details** command.

show wireless vlan details [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Examples

The following example shows how to see the VLAN details:

```
Device# show wireless vlan details chassis active r0
```

show wireless wgb mac-address

To view all the clients of the wireless workgroup bridge (WGB) using its MAC address, use the **show wireless wgb mac-address** command.

show wireless wgb mac-address *mac-address* **detail**

Syntax Description

mac-address MAC address of the WGB.

detail View clients of the wireless WGB.

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Examples

The following example shows how to see the clients of the wireless WGB:

```
Device# show wireless wgb mac-address 98-C7-7B-09-EF-ED detail
```

show wireless wgb summary

To see the active workgroup bridges (WGB), use the **show wireless wgb summary** command.

show wireless wgb summary

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Examples

The following example shows how to see the active workgroup bridges (WGB):

```
Device# show wireless wgb summary
```

show wireless wps mfp ap summary

To verify, if access points support Management Frame Protection (MFP) validation and protection, use the **show wireless wps mfp ap summary** command.

show wireless wps mfp ap summary

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC

Command History

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

This example shows the access points that support MFP validation and protection:

```
Device# show wireless wps mfp ap summary
AP Name                               Radio MAC                               Validation                               Protection
-----
AP002A.1087.CBF4                       00a2.eefd.bdc0                         Enabled                                  Enabled
AP58AC.78DE.9946                       00a2.eeb8.4ae0                         Enabled                                  Enabled
APb4de.3196.caac                       4c77.6d83.6b90                         Enabled                                  Enabled
```

show wireless wps mfp statistics

To view the Management Frame Protection (MFP) statistics, use the **show wireless wps mfp statistics** command.

show wireless wps mfp statistics

| | |
|---------------------------|--|
| Syntax Description | This command has no keywords or arguments. |
|---------------------------|--|

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

| | |
|----------------------|-----------------|
| Command Modes | Privileged EXEC |
|----------------------|-----------------|

| Command History | Release | Modification |
|------------------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.12.1 | This command was introduced. |

This example shows the Management Frame Protection (MFP) statistics:

```
Device# show wireless wps mfp statistics
BSSID          Radio DetectorAP          LastSourceAddr Error          Count
  FrameTypes
aabb.ccdd.eeff a      AP3800
  Beacon, Probe Response          aabb.ccdd.eeff Invalid MIC          10
                                   Invalid MIC          20
  Beacon, Probe Response
```

show wireless wps mfp summary

To view the detailed information of Management Frame Protection (MFP), use the **show wireless wps mfp summary** command.

show wireless wps mfp summary

| Syntax Description | This command has no keywords or arguments. | | | | |
|--------------------------------|--|---------|--------------|--------------------------------|------------------------------|
| Command Default | None | | | | |
| Command Modes | Privileged EXEC | | | | |
| Command History | <table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>Cisco IOS XE Gibraltar 16.12.1</td><td>This command was introduced.</td></tr></tbody></table> | Release | Modification | Cisco IOS XE Gibraltar 16.12.1 | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE Gibraltar 16.12.1 | This command was introduced. | | | | |

This example shows the detailed information of Management Frame Protection (MFP):

```
Device# show wireless wps mfp summary
Management Frame Protection
  Global Infrastructure MFP state : Enabled
  AP Impersonation detection    : Disabled
  Key refresh interval          : 15
```

show wireless wps rogue

To see the Rogue AP and Client information, use the **show wireless wps rogue** command.

See Adhoc Rogues (IBSS) information

show wireless wps rogue {adhoc | {detailed*mac-addr*} | summary}

See rogue AP information

show wireless wps rogueap {clients*mac-addr* | customsummary | detailed*mac-addr* | friendlysummary | list*mac-addressmac-addr* | malicious summary | summary | unclassifiedsummary | rldp {summary | in-progress | detailed*rogue-ap-mac-addr*}}

See rogue auto-containment information

show wireless wps rogueauto-contain

See rogue client information

show wireless wps rogueclient {summary | detailed*mac-addr*}

See rogue ignore list

show wireless wps rogueignore-list

See classification rule information

show wireless wps roguerule {detailed*rule-name* | summary}

See statistics about rogue feature

show wireless wps roguestats[{internal}]

Syntax Description

mac-address MAC address of the client.

Command Default

None

Command Modes

Privileged EXEC

Command History

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

Examples

The following example shows how to see the rogue feature statistics:

```
Device# show wireless wps rogue stats
```


show wireless wps rogue ap summary

To display a list of all rogue access points detected by the device, use the **show wireless wps rogue ap summary** command.

show wireless wps rogue ap summary

Command Default

None.

Command Modes

Privileged EXEC

Command History

Release

Modification

This command was introduced.

Usage Guidelines

None.

This example shows how to display a list of all rogue access points detected by the device:

```
Device# show wireless wps rogue ap summary
```

```
Rogue Location Discovery Protocol      : Disabled
Rogue on wire Auto-Contain             : Disabled
Rogue using our SSID Auto-Contain     : Disabled
Valid client on rogue AP Auto-Contain : Disabled
Rogue AP timeout                       : 1200
Rogue Detection Report Interval       : 10
Rogue AP minimum RSSI                 : -128
Rogue AP minimum transient time       : 0
```

```
Number of rogue APs detected : 624
```

| MAC Address | Classification | # APs | # Clients | Last Heard |
|----------------|----------------|-------|-----------|--------------------------|
| 0018.e78d.250a | Unclassified | 1 | 0 | Thu Jul 25 05:04:01 2013 |
| 0019.0705.d5bc | Unclassified | 1 | 0 | Thu Jul 25 05:16:26 2013 |
| 0019.0705.d5bd | Unclassified | 1 | 0 | Thu Jul 25 05:10:28 2013 |
| 0019.0705.d5bf | Unclassified | 1 | 0 | Thu Jul 25 05:16:26 2013 |

show wireless wps rogue client detailed

To view the detailed information of a specific rogue client, use the **show wireless wps rogue client detailed** *client-mac* command.

show wireless wps rogue client detailed *client-mac*

| | | |
|---------------------------|--|------------------------------|
| Syntax Description | <i>client-mac</i> MAC address of the rogue client. | |
| Command Default | None. | |
| Command Modes | Privileged EXEC | |
| Command History | Release | Modification |
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |
| Usage Guidelines | None. | |

This example shows how to display the detailed information for a specific rogue client:

```
Device# show wireless wps rogue client detail 0024.d7f1.2558
Rogue BSSID                : 64d8.146f.379f
Rogue Radio Type           : 802.11n - 5GHz
State                       : Alert
First Time Rogue was Reported : Wed Aug 7 12:51:43 2013
Last Time Rogue was Reported  : Wed Aug 7 12:51:43 2013
Reported by
  AP 2
    MAC Address             : 3cce.7309.0370
    Name                    : AP3502-talwar-ccie
    Radio Type              : 802.11a
    RSSI                    : -42 dBm
    SNR                     : 47 dB
    Channel                 : 52
    Last reported by this AP : Wed Aug 7 12:51:43 2013
```

show wireless wps rogue ap detailed

To view the detailed information of a rogue access point, use **show wireless wps rogue ap detailed** *mac-address* command.

show wireless wps rogue ap detailed 0008.30a7.7797

| | |
|---------------------------|--|
| Syntax Description | <i>mac-address</i> The MAC address of the rogue access point. |
| | Note If a rogue access point uses dot11n on 2.4GHz, the command output displays the radio type as dot11g , dot11n - 2.4 GHz . |

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

| | |
|----------------------|-----------------|
| Command Modes | Privileged EXEC |
|----------------------|-----------------|

| Command History | Release | Modification |
|------------------------|--------------------------|------------------------------|
| | Cisco IOS XE Fuji 16.7.x | This command was introduced. |

Example

This example shows how to display the detailed information about a rogue access point:

```
Device# wireless wps rogue ap detailed 0008.30a7.7797
Rogue Event history

Rogue BSSID                               : 0008.30a7.7797
Is Rogue on Wired Network                  : No
Classification                             : Unclassified
Manually Contained                         : Yes
State                                       : Contained Pending
Containment Level                           : 1
Number of Containing APs                   : 0
First Time Rogue was Reported              : 03/08/2017 17:41:55
Last Time Rogue was Reported               : 03/08/2017 21:48:34

Number of clients                           : 0

Reported By
  AP Name : JEWLC-AA
  MAC Address           : 00d7.8f4e.7240
  Detecting slot ID     : 0
  Radio Type            : dot11g , dot11n - 2.4 GHz
  SSID                  : psk
  Channel               : 5
  Channel Width         : 20 MHz
  RSSI                  : -128 dBm
  SNR                   : 0 dB
  Encryption            : Enabled
  ShortPreamble         : Disabled
  WPA Support           : Not Friendly
  Last reported by this AP : 03/08/2017 21:48:34
```

show wireless wps rogue client summary

To display summary of WPS rogue clients, use the **show wireless wps rogue client summary** command.

show wireless wps rogue client summary

Command Default None

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|--------------------------------|------------------------------|
| | Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

Usage Guidelines

Example

The following displays the output of the **show wireless wps rogue client summary** command:

```
Device# show wireless wps rogue client summary
Validate rogue clients against AAA : Disabled
Validate rogue clients against MSE : Enabled
Number of rogue clients detected : 0
```

show wireless wps summary

To view the detailed information of wps, use the **show wireless wps summary** command.

show wireless wps summary

| | | |
|---------------------------|--|---|
| Syntax Description | This command has no keywords or arguments. | |
| Command Default | None | |
| Command Modes | Privileged EXEC (#) | |
| Command History | Release | Modification |
| | Cisco IOS XE Gibraltar 16.12.1 | This command was introduced. |
| | Cisco IOS XE Amsterdam 17.3.5 | The output of the command was modified to include ARP activity information. |

This example shows if the Management Frame Protection (MFP) is enabled or disabled:

```
Device# show wireless wps summary

Client Exclusion Policy
  Excessive 802.11-association failures   : unknown
  Excessive 802.11-authentication failures: unknown
  Excessive 802.1x-authentication         : unknown
  IP-theft                                : unknown
  Excessive Web authentication failure    : unknown
  Failed Qos Policy                       : unknown

Management Frame Protection
  Global Infrastructure MFP state         : Enabled
  AP Impersonation detection             : Disabled
  Key refresh interval                   : 15
```

This example shows whether rate limiting is enabled for ARP packets:

```
Device# show wireless wps summary

Client Exclusion Policy
  Excessive 802.11-association failures   : Enabled
  Excessive 802.1x-authentication         : Enabled
  Mac and IP-theft                       : Enabled
  Excessive Web authentication failure    : Enabled
  Failed Qos Policy                       : Enabled
  Excessive ARP Activity                   : Enabled (per policy setting)
```

show wlan name client stats

To view the WLAN client statistics, use the **show wlan name client stats** command.

show wlan name *wlan-name* **client stats**

| Syntax Description | <i>wlan-name</i> WLAN name. | | | | |
|--------------------------------|--|---------|--------------|--------------------------------|------------------------------|
| Command Default | None | | | | |
| Command Modes | Privileged EXEC(#) | | | | |
| Command History | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Amsterdam 17.1.1s</td> <td>This command was introduced.</td> </tr> </tbody> </table> | Release | Modification | Cisco IOS XE Amsterdam 17.1.1s | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE Amsterdam 17.1.1s | This command was introduced. | | | | |

This example shows how to view the WLAN client statistics:

```
Device# show wlan name wlan1 client stats
```

```
Wlan Profile Name: wlan1, Wlan Id: 3
```

```
Current client state statistics:
```

```
-----
Authenticating      : 0
Mobility            : 0
IP Learn            : 0
Webauth Pending    : 0
Run                 : 0
```

```
Locally Administered MAC Clients : 0
```

```
L3 Access Clients      : 0
```

```
.
.
.
```

show wlan summary sort ascending client-count

To view the WLAN summary sorted ascendingly based on the client count, use the **show wlan summary sort ascending client-count** command.

show wlan summary sort ascending client-count

| Syntax Description | This command has no keywords or arguments. | | | | |
|--------------------------------|--|---------|--------------|--------------------------------|------------------------------|
| Command Default | None | | | | |
| Command Modes | Privileged EXEC | | | | |
| Command History | <table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>Cisco IOS XE Amsterdam 17.1.1s</td><td>This command was introduced.</td></tr></tbody></table> | Release | Modification | Cisco IOS XE Amsterdam 17.1.1s | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE Amsterdam 17.1.1s | This command was introduced. | | | | |

This example shows how to view the WLAN summary sorted ascendingly based on the client count:

```
Device# show wlan summary sort ascending client-count
```

```
-----  
Wlan-name                               ID           Client count      Data Usage  
-----  
r1an_test_1                             1            1                  6277  
WLAN_CA_WPA2_AES_DOT1X                 70           1                  167781  
-----
```

show wlan summary sort descending client-count

To view the WLAN summary sorted descendingly based on the client count, use the **show wlan summary sort descending client-count** command.

show wlan summary sort descending client-count

| | | |
|---------------------------|--|------------------------------|
| Syntax Description | This command has no keywords or arguments. | |
| Command Default | None | |
| Command Modes | Privileged EXEC | |
| Command History | Release | Modification |
| | Cisco IOS XE Amsterdam 17.1.1s | This command was introduced. |

This example shows how to view the WLAN summary sorted descendingly based on the client count:

```
Device# show wlan summary sort descending client-count
```

```
-----
Wlan-name                ID           Client count      Data Usage
-----
rlan_test_1              1            1                  6277
WLAN_CA_WPA2_AES_DOT1X  70           1                  167781
-----
```


show wlan summary sort ascending data-usage

To view the wlan summary sorted ascendingly based on the data usage, use the **show wlan summary sort ascending data-usage** command.

show wlan summary sort ascending data-usage

| Syntax Description | This command has no keywords or arguments. | | | | |
|-------------------------------|---|---------|--------------|-------------------------------|------------------------------|
| Command Default | None | | | | |
| Command Modes | Privileged EXEC | | | | |
| Command History | <table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>Cisco IOS XE Gibraltar 17.1.1</td><td>This command was introduced.</td></tr></tbody></table> | Release | Modification | Cisco IOS XE Gibraltar 17.1.1 | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE Gibraltar 17.1.1 | This command was introduced. | | | | |

This example shows how to view the wlan summary sorted ascendingly based on the data usage:

```
Device# show wlan summary sort ascending data-usage
```

```
-----  
Wlan-name                ID          Client count    Data Usage  
-----  
r1an_test_1              1           1                6277  
WLAN_CA_WPA2_AES_DOT1X  70          1                167781  
-----
```

show wlan summary sort descending data-usage

To view the WLAN summary sorted descendingly based on the data usage, use the **show wlan summary sort descending data-usage** command.

show wlan summary sort descending data-usage

| | | |
|---------------------------|--|------------------------------|
| Syntax Description | This command has no keywords or arguments. | |
| Command Default | None | |
| Command Modes | Privileged EXEC | |
| Command History | Release | Modification |
| | Cisco IOS XE Amsterdam 17.1.1s | This command was introduced. |

This example shows how to view the WLAN summary sorted descendingly based on the data usage:

```
Device# show wlan summary sort descending data-usage
```

```
-----
Wlan-name                ID           Client count      Data Usage
-----
WLAN_CA_WPA2_AES_DOT1X   70           1                  167781
rln_test_1                1            1                  6277
-----
```

show wps summary

To display Wireless Protection System (WPS) summary information, use the **show wps summary** command.

show wps summary

| Syntax Description | Description |
|--------------------|--|
| | This command has no arguments or keywords. |
| Command Default | None |

The following example shows how to display WPS summary information:

```
(Cisco Controller) > show wps summary
Auto-Immune
  Auto-Immune..... Disabled
Client Exclusion Policy
  Excessive 802.11-association failures..... Enabled
  Excessive 802.11-authentication failures..... Enabled
  Excessive 802.1x-authentication..... Enabled
  IP-theft..... Enabled
  Excessive Web authentication failure..... Enabled
Trusted AP Policy
  Management Frame Protection..... Disabled
  Mis-configured AP Action..... Alarm Only
    Enforced encryption policy..... none
    Enforced preamble policy..... none
    Enforced radio type policy..... none
  Validate SSID..... Disabled
  Alert if Trusted AP is missing..... Disabled
  Trusted AP timeout..... 120
Untrusted AP Policy
  Rogue Location Discovery Protocol..... Disabled
    RLDP Action..... Alarm Only
Rogue APs
  Rogues AP advertising my SSID..... Alarm Only
  Detect and report Ad-Hoc Networks..... Enabled
Rogue Clients
  Validate rogue clients against AAA..... Enabled
  Detect trusted clients on rogue APs..... Alarm Only
  Rogue AP timeout..... 1300
Signature Policy
  Signature Processing..... Enabled
...
```

shutdown

To close the RF Profile and disable the network, use the **shutdown** command. To disable shutdown execution, use the **no** form of this command.

shutdown

| | | |
|---------------------------|----------------------------|--|
| Syntax Description | shutdown | Shuts down the profile and disables network. |
| Command Default | None | |
| Command Modes | config-rf-profile | |
| Command History | Release | Modification |
| | Cisco IOS XE Denali 16.3.1 | This command was introduced. |
| Usage Guidelines | None | |

This example shows how to close a RF Profile and disable the network.

```
Device (config-rf-profile) #shutdown
```