THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2019 Cisco Systems, Inc. All rights reserved.
## CONTENTS

### PREFACE

- Preface xxiii
  - Document Conventions xxiii
  - Related Documentation xxv
  - Obtaining Documentation and Submitting a Service Request xxv

### CHAPTER 1

- Using the Command-Line Interface 1
  - Information About Using the Command-Line Interface 2
    - Command Modes 2
    - Understanding Abbreviated Commands 4
    - No and Default Forms of Commands 4
    - CLI Error Messages 4
    - Configuration Logging 5
    - Using the Help System 5

### CHAPTER 2

- Configuration Commands: a to f 7
  - aaa accounting identity 12
  - aaa accounting update periodic interval-in-minutes 14
  - aaa authentication dot1x 15
  - aaa authentication login 16
  - aaa authorization 17
  - aaa authorization credential download default 21
  - aaa group server ldap 22
  - aaa group server radius 23
  - aaa local authentication default authorization 24
  - aaa new-model 25
  - aaa server radius dynamic-author 27
device-tracking policy 231
dhcp-tlv-caching 233
dns-server (IPv6) 234
dnscrypt 235
domain-name (DHCP) 236
dot11 airtime-fairness 237
dot11 5ghz reporting-interval 238
dot11 reporting-interval 239
dot1x system-auth-control 240
eap profile 242
et-analytics 243
ethernet-vlan-transparent (mesh) 244
ethernet-bridging (mesh) 245
event identity-update 246
exclusionlist 247
fabric control-plane 248
fallback-radio-shut 249
flex 250
flow exporter 251
flow monitor 252
flow record 253
full-sector-dfs (mesh) 254

CHAPTER 3

Configuration Commands: g to z 255

hyperlocation 261
idle-timeout 262
ids (mesh) 263
inactive-timeout 264
interface vlan 265
ip access-group 266
ip access-list extended 267
ip address 268
ip admission 271
ip dhcp pool 272
wireless mobility multicast ipv4  536
wireless mobility mac-address  537
wireless multicast  538
wireless profile airtime-fairness  539
wireless profile ap packet-capture  540
wireless profile fabric  541
wireless profile policy  542
wireless rfid  543
wireless security dot1x  544
wireless security dot1x radius accounting mac-delimiter  546
wireless security dot1x radius accounting username-delimiter  547
wireless security dot1x radius callStationIdCase  548
wireless security dot1x radius mac-authentication call-station-id  549
wireless security dot1x radius mac-authentication mac-delimiter  550
wireless security web-auth retries  551
wireless tag policy  552
wireless tag site  553
wireless wps ap-authentication  554
wireless wps client-exclusion  555
wireless wps rogue  557
wireless wps rogue ap rldp alarm-only  558
wireless wps rogue ap rldp auto-contain  559
wireless wps rogue client  560
wireless wps rogue detection  561
wireless wps rogue rule  562
wireless-default radius server  564
wlan policy  565

CHAPTER 4

Show Commands  567
show access-list  572
show ap airtime-fairness summary  574
show ap auth-list  575
show ap auto-rf  576
show ap config  578
show ap crash-file 579
show ap dot11 580
show ap dot11 586
show ap dot11 24ghz 587
show ap dot11 24ghz SI config 589
show ap dot11 24ghz SI device type 590
show ap dot11 5ghz 591
show ap dot11 clean air-quality 593
show ap dot11 cleanair config 594
show ap dot11 cleanair summary 596
show ap environment 597
show ap filters active 598
show ap filters all 599
show ap fra 600
show ap gps location 601
show ap group hyperlocation 602
show ap hyperlocation 604
show ap hyperlocation cmx summary 606
show ap image 607
show ap link-encryption 608
show ap master list 609
show ap monitor-mode summary 610
show ap name auto-rf 611
show ap name cablemodem 614
show ap name config 615
show ap name config ethernet 617
show ap name dot11 618
show ap name environment 621
show ap name gps location 622
show ap name hyperlocation 623
show ap name mesh backhaul 624
show ap name mesh bhrate 625
show ap name mesh linktest 626
show ap name mesh neighbor detail 627
show ap name mesh path 628
show ap name mesh stats 629
show ap name wlan 630
show ap profile 632
show ap rf-profile name 633
show ap rf-profile summary 635
show ap summary 636
show ap tag sources 637
show ap tag summary 638
show ap upgrade 639
show arp 640
show arp summary 641
show avc client 642
show avc wlan 643
show chassis 644
show checkpoint 645
show etherchannel summary 652
show flow exporter 653
show flow interface 655
show flow monitor 657
show flow record 659
show interfaces 660
show ip 664
show ip device tracking 665
show ip igmp snooping igmpv2-tracking 667
show ip igmp snooping querier 668
show ip igmp snooping wireless mcast-spi-count 670
show ip igmp snooping wireless mgid 671
show ip nbar protocol-discovery wlan 672
show ipv6 access-list 673
show ipv6 mld snooping 676
show ipv6 mld snooping querier vlan 678
show ipv6 mld snooping wireless mgid 679
show ldap attributes 680
show ldap server  681
show lisp site detail  682
show logging profile wireless end timestamp  683
show logging profile wireless filter  684
show logging profile wireless fru  685
show logging profile wireless internal  686
show logging profile wireless level  687
show logging profile wireless module  688
show logging profile wireless reverse  689
show logging profile wireless start  690
show logging profile wireless switch  691
show logging profile wireless to-file  692
show mac access-group  693
show mobility  694
show nmsp  696
show nmsp cloud-services statistics  697
show nmsp cloud-services summary  698
show nmsp subscription group detail ap-list  699
show nmsp subscription group detail services  700
show nmsp subscription group summary  701
show platform conditions  702
show platform hardware  703
show platform hardware chassis active qfp feature dns-snoop-agent client enabled-intf  704
show platform hardware chassis active qfp feature dns-snoop-agent client hw-pattern-list  705
show platform hardware chassis active qfp feature dns-snoop-agent client info  706
show platform hardware chassis active qfp feature dns-snoop-agent client pattern-list  707
show platform hardware chassis active qfp feature dns-snoop-agent datapath ip-cache  708
show platform hardware chassis active qfp feature dns-snoop-agent datapath memory  709
show platform hardware chassis active qfp feature dns-snoop-agent datapath regexp-table  710
show platform hardware chassis active qfp feature dns-snoop-agent datapath stats  711
show platform hardware chassis active qfp feature et-analytics datapath runtime  712
show platform hardware chassis active qfp feature et-analytics datapath memory  713
show platform hardware chassis active qfp feature et-analytics datapath stats export  714
show platform hardware chassis active qfp feature et-analytics datapath stats flow  715
show platform hardware chassis active qfp feature wireless et-analytics eta-pending-client-tree 716
show platform hardware chassis active qfp feature wireless et-analytics statistics 717
show platform software trace filter-binary 718
show platform software trace filter-binary 719
show platform software trace level 720
show platform software trace message 723
show platform software trace message license-manager RP 727
show platform software trace message license-manager 730
show platform software utd chassis active F0 et-analytics global 733
show platform software et-analytics global 734
show parameter-map type umbrella global 735
show policy-map 736
show redundancy 741
show remote-lan all 745
show remote-lan id 746
show remote-lan name 747
show remote-lan policy detail 748
show remote-lan policy summary 750
show remote-lan summary 751
show ssh 752
show tech wireless client 753
show tech-support wireless 757
show tech-support wireless ap 759
show tech-support wireless client 769
show tech-support wireless datapath 773
show tech-support wireless fabric 794
show tech-support wireless mobility 795
show tech-support wireless radio 807
show umbrella config 818
show umbrella deviceid 819
show umbrella deviceid detailed 820
show umbrella dnsencrypt 821
show vlan 822
show vlan access-map 825
show vlan filter  826
show vlan group  827
show wireless band-select  828
show wireless client  829
show wireless client mac-address  830
show wireless client mac-address (Call Control)  831
show wireless client mac-address (TCLAS)  832
show wireless client mac-address mobility history  833
show wireless client summary  834
show wireless client timers  835
show wireless country  836
show wireless detail  839
show wireless dot11h  840
show wireless dtls connections  841
show wireless exclusionlist  842
show wireless fabric summary  843
show wireless fabric client summary  844
show wireless fabric vnid mapping  845
show wireless flow-control  846
show wireless flow-control statistics  847
show wireless load-balancing  848
show wireless media-stream client detail  849
show wireless media-stream group  850
show wireless media-stream message details  851
show wireless mobility controller ap  852
show wireless media-stream multicast-direct state  853
show wireless mesh ap  854
show wireless mesh ap summary  855
show wireless mesh ap tree  856
show wireless mesh ap tree  857
show wireless mesh config  858
show wireless mesh neighbor  859
show wireless mobility  860
show wireless mobility peer ip  861
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show wireless multicast group summary</td>
<td>862</td>
</tr>
<tr>
<td>show wireless mobility summary</td>
<td>863</td>
</tr>
<tr>
<td>show wireless multicast</td>
<td>864</td>
</tr>
<tr>
<td>show wireless multicast group</td>
<td>865</td>
</tr>
<tr>
<td>show wireless performance</td>
<td>866</td>
</tr>
<tr>
<td>show wireless pmk-cache</td>
<td>867</td>
</tr>
<tr>
<td>show wireless probe</td>
<td>868</td>
</tr>
<tr>
<td>show wireless profile airtime-fairness mapping</td>
<td>869</td>
</tr>
<tr>
<td>show wireless profile airtime-fairness summary</td>
<td>870</td>
</tr>
<tr>
<td>show wireless profile ap packet-capture</td>
<td>871</td>
</tr>
<tr>
<td>show wireless profile fabric detailed</td>
<td>873</td>
</tr>
<tr>
<td>show wireless profile flex</td>
<td>874</td>
</tr>
<tr>
<td>show wireless redundancy statistics</td>
<td>875</td>
</tr>
<tr>
<td>show wireless rfid</td>
<td>876</td>
</tr>
<tr>
<td>show wireless statistics mobility</td>
<td>877</td>
</tr>
<tr>
<td>show wireless stats mesh packet error</td>
<td>878</td>
</tr>
<tr>
<td>show wireless stats mesh security and queue</td>
<td>879</td>
</tr>
<tr>
<td>show wireless summary</td>
<td>880</td>
</tr>
<tr>
<td>show wireless tag rf</td>
<td>881</td>
</tr>
<tr>
<td>show wireless urlfilter details</td>
<td>882</td>
</tr>
<tr>
<td>show wireless urlfilter summary</td>
<td>883</td>
</tr>
<tr>
<td>show wireless vlan details</td>
<td>884</td>
</tr>
<tr>
<td>show wireless wgb mac-address</td>
<td>885</td>
</tr>
<tr>
<td>show wireless wgb summary</td>
<td>886</td>
</tr>
<tr>
<td>show wireless wps rogue</td>
<td>887</td>
</tr>
<tr>
<td>show wireless wps rogue ap summary</td>
<td>888</td>
</tr>
<tr>
<td>show wireless wps rogue client detailed</td>
<td>889</td>
</tr>
<tr>
<td>show wireless wps rogue client summary</td>
<td>890</td>
</tr>
<tr>
<td>show wps summary</td>
<td>891</td>
</tr>
<tr>
<td>shutdown</td>
<td>893</td>
</tr>
</tbody>
</table>
Preface

- Document Conventions, on page xxiii
- Related Documentation, on page xxv
- Obtaining Documentation and Submitting a Service Request, on page xxv

Document Conventions

This document uses the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>^ or Ctrl</td>
<td>Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination ^D or Ctrl-D means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.)</td>
</tr>
<tr>
<td><strong>bold</strong> font</td>
<td>Commands and keywords and user-entered text appear in <strong>bold</strong> font.</td>
</tr>
<tr>
<td><em>Italic</em> font</td>
<td>Document titles, new or emphasized terms, and arguments for which you supply values are in <em>italic</em> font.</td>
</tr>
<tr>
<td><strong>Courier</strong> font</td>
<td>Terminal sessions and information the system displays appear in <strong>courier</strong> font.</td>
</tr>
<tr>
<td><strong>Bold Courier</strong> font</td>
<td><strong>Bold Courier</strong> font indicates text that the user must enter.</td>
</tr>
<tr>
<td>[x]</td>
<td>Elements in square brackets are optional.</td>
</tr>
<tr>
<td>...</td>
<td>An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>[x</td>
<td>y]</td>
</tr>
<tr>
<td>{x</td>
<td>y}</td>
</tr>
<tr>
<td>Convention</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>[x {y</td>
<td>z}]</td>
</tr>
<tr>
<td>string</td>
<td>A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.</td>
</tr>
<tr>
<td>&lt; : &gt;</td>
<td>Nonprinting characters such as passwords are in angle brackets.</td>
</tr>
<tr>
<td>[]</td>
<td>Default responses to system prompts are in square brackets.</td>
</tr>
<tr>
<td>!, #</td>
<td>An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.</td>
</tr>
</tbody>
</table>

**Reader Alert Conventions**

This document may use the following conventions for reader alerts:

**Note**

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

**Tip**

Means *the following information will help you solve a problem*.

**Caution**

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

**Timesaver**

Means *the described action saves time*. You can save time by performing the action described in the paragraph.

**Warning**

**IMPORTANT SAFETY INSTRUCTIONS**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS
Related Documentation

Before installing or upgrading the device, refer to the device release notes.

- Cisco Catalyst 9800-40 Wireless Controller documentation, located at:
  http://www.cisco.com/go/c9800
- Cisco Catalyst 9800-80 Wireless Controller documentation, located at:
  http://www.cisco.com/go/c9800

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:


Subscribe to the What's New in Cisco Product Documentation as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.
Obtaining Documentation and Submitting a Service Request
Using the Command-Line Interface

- Information About Using the Command-Line Interface, on page 2
Information About Using the Command-Line Interface

Note
Search options on the GUI and CLI are case sensitive.

Command Modes

The Cisco IOS user interface is divided into many different modes. The commands available to you depend on which mode you are currently in. Enter a question mark (?) at the system prompt to obtain a list of commands available for each command mode.

You can start a CLI session through a console connection, through Telnet, an SSH, or by using the browser. When you start a session, you begin in user mode, often called user EXEC mode. Only a limited subset of the commands are available in user EXEC mode. For example, most of the user EXEC commands are one-time commands, such as `show` commands, which show the current configuration status, and `clear` commands, which clear counters or interfaces. The user EXEC commands are not saved when the device reboots.

To have access to all commands, you must enter privileged EXEC mode. Normally, you must enter a password to enter privileged EXEC mode. From this mode, you can enter any privileged EXEC command or enter global configuration mode.

Using the configuration modes (global, interface, and line), you can make changes to the running configuration. If you save the configuration, these commands are stored and used when the device reboots. To access the various configuration modes, you must start at global configuration mode. From global configuration mode, you can enter interface configuration mode and line configuration mode.

This table describes the main command modes, how to access each one, the prompt you see in that mode, and how to exit the mode.

Table 1: Command Mode Summary

<table>
<thead>
<tr>
<th>Mode</th>
<th>Access Method</th>
<th>Prompt</th>
<th>Exit Method</th>
<th>About This Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>User EXEC</td>
<td>Begin a session using Telnet, SSH, or console.</td>
<td>Device&gt;</td>
<td>Enter <code>logout</code> or <code>quit</code>.</td>
<td>Use this mode to:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Change terminal settings.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Perform basic tests.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Display system information.</td>
</tr>
<tr>
<td>Mode</td>
<td>Access Method</td>
<td>Prompt</td>
<td>Exit Method</td>
<td>About This Mode</td>
</tr>
<tr>
<td>----------------------</td>
<td>----------------------------------------------------</td>
<td>------------------</td>
<td>------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td>While in user EXEC mode, enter the enable command.</td>
<td>Device#</td>
<td>Enter disable to exit.</td>
<td>Use this mode to verify commands that you have entered. Use a password to protect access to this mode.</td>
</tr>
<tr>
<td>Global configuration</td>
<td>While in privileged EXEC mode, enter the configure command.</td>
<td>Device(config)#</td>
<td>To exit to privileged EXEC mode, enter exit or end, or press Ctrl-Z.</td>
<td>Use this mode to configure parameters that apply to the entire device.</td>
</tr>
<tr>
<td>VLAN configuration</td>
<td>While in global configuration mode, enter the vlan vlan-id command.</td>
<td>Device(config-vlan)#</td>
<td>To exit to global configuration mode, enter the exit command. To return to privileged EXEC mode, press Ctrl-Z or enter end.</td>
<td>Use this mode to configure VLAN parameters. When VTP mode is transparent, you can create extended-range VLANs (VLAN IDs greater than 1005) and save configurations in the device startup configuration file.</td>
</tr>
<tr>
<td>Interface configuration</td>
<td>While in global configuration mode, enter the interface command (with a specific interface).</td>
<td>Device(config-if)#</td>
<td>To exit to global configuration mode, enter exit. To return to privileged EXEC mode, press Ctrl-Z or enter end.</td>
<td>Use this mode to configure parameters for the Ethernet ports.</td>
</tr>
<tr>
<td>Line configuration</td>
<td>While in global configuration mode, specify a line with the line vty or line console command.</td>
<td>Device(config-line)#</td>
<td>To exit to global configuration mode, enter exit. To return to privileged EXEC mode, press Ctrl-Z or enter end.</td>
<td>Use this mode to configure parameters for the terminal line.</td>
</tr>
</tbody>
</table>
Understanding Abbreviated Commands

You need to enter only enough characters for the device to recognize the command as unique.

This example shows how to enter the `show configuration` privileged EXEC command in an abbreviated form:

```
Device# show conf
```

No and Default Forms of Commands

Almost every configuration command also has a `no` form. In general, use the `no` form to disable a feature or function or reverse the action of a command. For example, the `no shutdown` interface configuration command reverses the shutdown of an interface. Use the command without the keyword `no` to reenable a disabled feature or to enable a feature that is disabled by default.

Configuration commands can also have a `default` form. The `default` form of a command returns the command setting to its default. Most commands are disabled by default, so the `default` form is the same as the `no` form. However, some commands are enabled by default and have variables set to certain default values. In these cases, the `default` command enables the command and sets variables to their default values.

CLI Error Messages

This table lists some error messages that you might encounter while using the CLI to configure your device.

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Meaning</th>
<th>How to Get Help</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>% Ambiguous command: &quot;show con&quot;</code></td>
<td>You did not enter enough characters for your device to recognize the command.</td>
<td>Reenter the command followed by a question mark (?) without any space between the command and the question mark.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The possible keywords that you can enter with the command appear.</td>
</tr>
<tr>
<td><code>% Incomplete command.</code></td>
<td>You did not enter all of the keywords or values required by this command.</td>
<td>Reenter the command followed by a question mark (?) with a space between the command and the question mark.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The possible keywords that you can enter with the command appear.</td>
</tr>
<tr>
<td><code>% Invalid input detected at </code>^<code> marker.</code></td>
<td>You entered the command incorrectly. The caret (^) marks the point of the error.</td>
<td>Enter a question mark (?) to display all of the commands that are available in this command mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The possible keywords that you can enter with the command appear.</td>
</tr>
</tbody>
</table>
Configuration Logging

You can log and view changes to the device configuration. You can use the Configuration Change Logging and Notification feature to track changes on a per-session and per-user basis. The logger tracks each configuration command that is applied, the user who entered the command, the time that the command was entered, and the parser return code for the command. This feature includes a mechanism for asynchronous notification to registered applications whenever the configuration changes. You can choose to have the notifications sent to the syslog.

Note

Only CLI or HTTP changes are logged.

Using the Help System

You can enter a question mark (?) at the system prompt to display a list of commands available for each command mode. You can also obtain a list of associated keywords and arguments for any command.

SUMMARY STEPS

1. help
2. abbreviated-command-entry ?
3. abbreviated-command-entry <Tab>
4. ?
5. command ?
6. command keyword ?

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>help</td>
<td>Obtains a brief description of the help system in any command mode.</td>
</tr>
<tr>
<td>Example: Device# help</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>abbreviated-command-entry ?</td>
<td>Obtains a list of commands that begin with a particular character string.</td>
</tr>
<tr>
<td>Example: Device# di? dir disable disconnect</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>abbreviated-command-entry &lt;Tab&gt;</td>
<td>Completes a partial command name.</td>
</tr>
<tr>
<td>Example: Device# sh conf&lt;tab&gt; Device# show configuration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>?</td>
<td>Lists all commands available for a particular command mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><strong>Device&gt; ?</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Step 5**

**command ?**

*Example:*

Device> show ?

Lists the associated keywords for a command.

**Step 6**

**command keyword ?**

*Example:*

Device(config)# cdp holdtime ?

- <10-255> Length of time (in sec) that receiver must keep this packet

Lists the associated arguments for a keyword.
Configuration Commands: a to f

• aaa accounting identity, on page 12
• aaa accounting update periodic interval-in-minutes , on page 14
• aaa authentication dot1x, on page 15
• aaa authentication login, on page 16
• aaa authorization, on page 17
• aaa authorization credential download default, on page 21
• aaa group server ldap, on page 22
• aaa group server radius, on page 23
• aaa local authentication default authorization, on page 24
• aaa new-model, on page 25
• aaa server radius dynamic-author, on page 27
• aaa session-id, on page 29
• aaa-override, on page 31
• aaa-policy , on page 32
• aaa-realm enable , on page 33
• absolute-timer, on page 34
• access-list, on page 35
• access-list acl-ace-limit, on page 37
• accounting-list, on page 38
• acl-policy, on page 39
• address, on page 40
• address prefix, on page 42
• airtime-fairness mode, on page 43
• allow at-least min-number at-most max-number, on page 44
• amsdu (mesh), on page 45
• ap, on page 46
• ap auth-list ap-policy, on page 47
• ap auth-list ap-policy, on page 48
• ap capwap backup, on page 49
• ap capwap multicast, on page 50
• ap capwap retransmit, on page 51
• ap capwap timers, on page 52
• ap cdp, on page 54
• ap country, on page 55
• ap dot11, on page 56
• ap dot11 24ghz cleanair, on page 57
• default ap dot11 24ghz cleanair device, on page 58
• ap dot11 24ghz dot11g, on page 60
• ap dot11 24ghz rate, on page 61
• ap dot11 24ghz rrm optimized-roam, on page 63
• ap dot11 rrm channel cleanair-event, on page 64
• ap dot11 24ghz rrm channel cleanair-event, on page 65
• ap dot11 24ghz rrm channel device, on page 66
• ap dot11 24ghz rx-sop threshold, on page 67
• ap dot11 5ghz channelswitch mode, on page 68
• ap dot11 5ghz channelswitch quiet, on page 69
• ap dot11 5ghz cleanair, on page 70
• default ap dot11 5ghz cleanair device, on page 71
• ap dot11 5ghz dot11ac frame-burst automatic, on page 72
• ap dot11 5ghz power-constraint, on page 73
• ap dot11 5ghz rate, on page 74
• ap dot11 5ghz rrm channel cleanair-event, on page 75
• ap dot11 5ghz rrm channel device, on page 76
• ap dot11 5ghz channelswitch mode, on page 77
• ap dot11 5ghz rx-sop threshold, on page 78
• ap dot11 5ghz shutdown, on page 79
• ap dot11 5ghz smart-dfs, on page 80
• ap dot11 beaconperiod, on page 81
• ap dot11 cac media-stream, on page 82
• ap dot11 cac multimedia, on page 85
• ap dot11 cac video, on page 86
• ap dot11 cac voice, on page 88
• ap dot11 cleanair, on page 91
• ap dot11 cleanair device, on page 92
• ap dot11 dot11n, on page 94
• ap dot11 dpc, on page 97
• ap dot11 edca-parameters, on page 99
• ap dot11 rf-profile, on page 100
• ap dot11 rf-profile, on page 101
• ap dot11 rrm, on page 102
• ap dot11 rrm channel, on page 105
• ap dot11 rrm channel dca, on page 106
• ap dot11 rrm coverage, on page 108
• ap dot11 rrm group-member, on page 110
• ap dot11 rrm group-mode, on page 111
• ap dot11 rrm logging, on page 112
• ap dot11 rrm monitor, on page 114
• ap dot11 rrm ndp-type, on page 115
• ap dot11 rrm tpc-threshold, on page 116
• ap dot11 rrm txpower, on page 117
• ap dot11 rrm txpower, on page 118
• ap filter , on page 119
• ap fra, on page 120
• ap hyperlocation, on page 121
• ap image, on page 122
• ap image upgrade, on page 123
• ap link-encryption, on page 124
• ap name clear-personal-ssid, on page 125
• ap name core-dump, on page 126
• ap name crash-file, on page 127
• ap name dot11 dual-band cleanair, on page 128
• ap name dot11 dual-band shutdown, on page 129
• ap name dot11 rrm profile, on page 130
• ap name hyperlocation, on page 132
• ap name mesh block-child, on page 133
• ap name mesh daisy-chaining, on page 134
• ap name mesh ethernet mode access, on page 135
• ap name mesh ethernet mode trunk, on page 136
• ap name mesh linktest, on page 137
• ap name mesh parent preferred, on page 138
• ap name mesh security psk provisioning delete, on page 139
• ap name mesh vlan-trunking native, on page 140
• ap name mesh vlan-trunking native, on page 141
• ap name mode, on page 142
• ap name mode bridge, on page 144
• ap name monitor-mode, on page 145
• ap name monitor-mode dot11b, on page 146
• ap name priority, on page 147
• ap name role, on page 148
• ap name shutdown, on page 149
• ap name sniff, on page 150
• ap name tftp-downgrade, on page 151
• ap name vlan-tag, on page 152
• ap name write tag-config , on page 153
• ap name-regex , on page 154
• ap packet-capture, on page 155
• ap packet-capture profile, on page 156
• ap packet-capture start, on page 157
• ap profile, on page 158
• ap remote-lan profile-name, on page 159
• ap remote-lan shutdown, on page 160
• ap remote-lan-policy policy-name, on page 161
• ap tag-source-priority , on page 162
• ap tag-sources revalidate , on page 163
• ap vlan-tag, on page 164
• arp-caching, on page 165
• assisted-roaming, on page 166
• auto qos, on page 167
• avg-packet-size packetsize, on page 168
• Avoid label exhaustion error, on page 169
• backhaul (mesh), on page 170
• background-scanning (mesh), on page 171
• band-select client, on page 172
• band-select cycle, on page 173
• band-select expire, on page 174
• band-select probe-response, on page 175
• bridge-group, on page 176
• bss-transition, on page 177
• battery-state (mesh), on page 178
• cache timeout active value, on page 179
• cache timeout inactive value, on page 180
• call-snoop, on page 181
• captive-portal-bypass, on page 182
• ccn (mesh), on page 183
• central association, on page 184
• central authentication, on page 185
• central dhcp, on page 186
• central switching, on page 187
• central-webauth, on page 188
• chassis clear, on page 189
• chassis ha-interface, on page 190
• chassis priority, on page 191
• chassis timer peer-timeout, on page 192
• class, on page 193
• classify, on page 196
• class-map, on page 197
• clear ip nbar protocol-discovery wlan, on page 199
• clear platform condition all, on page 200
• clear subscriber policy peer, on page 201
• client-access (mesh), on page 202
• client association limit, on page 203
• channel foreign, on page 205
• client-12-vnid, on page 206
• collect counter, on page 207
• collect wireless ap mac address (wireless), on page 208
• collect wireless client mac address (wireless), on page 209
• convergence, on page 210
• coverage, on page 211
• crypto key generate rsa, on page 212
• cts inline-tagging, on page 218
• cts role-based enforcement, on page 219
• cts sgt, on page 220
• custom-page login device, on page 221
• default, on page 222
• debug platform qos-acl-tcam, on page 224
• debug qos-manager, on page 225
• description, on page 226
• destination, on page 227
• device-role (IPv6 snooping), on page 228
• device-role (IPv6 nd inspection), on page 229
• device-tracking binding vlan, on page 230
• device-tracking policy, on page 231
• dhcp-tlv-caching, on page 233
• dns-server (IPv6), on page 234
• dnscrypt, on page 235
• domain-name (DHCP), on page 236
• dot11 airtime-fairness, on page 237
• dot11 5ghz reporting-interval , on page 238
• dot11 reporting-interval, on page 239
• dot1x system-auth-control, on page 240
• eap profile, on page 242
• et-analytics, on page 243
• ethernet-vlan-transparent (mesh), on page 244
• ethernet-bridging (mesh), on page 245
• event identity-update, on page 246
• exclusionlist, on page 247
• fabric control-plane, on page 248
• fallback-radio-shut, on page 249
• flex , on page 250
• flow exporter, on page 251
• flow monitor, on page 252
• flow record, on page 253
• full-sector-dfs (mesh), on page 254
**aaa accounting identity**

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

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

**Syntax Description**

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

The `group` keyword is optional when you enter it after the `broadcast group` and `group` keywords. You can enter more than optional `group` keyword.

- `radius` (Optional) Enables RADIUS authorization.
- `tacacs+` (Optional) Enables TACACS+ accounting.

**Command Default**

- AAA accounting is disabled.

**Command Modes**

- Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To enable AAA accounting identity, you need to enable policy mode. To enable policy mode, enter the `authentication display new-style` command in privileged EXEC mode.
This example shows how to configure IEEE 802.1x accounting identity:

Device# authentication display new-style

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

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

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

Device# configure terminal
Device(config)# aaa accounting identity default start-stop group radius
aaa accounting update periodic interval-in-minutes

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

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

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>periodic</td>
<td>Send accounting update records at regular intervals.</td>
</tr>
<tr>
<td>&lt;1-71582&gt;</td>
<td>Periodic intervals to send accounting update records(in minutes)</td>
</tr>
<tr>
<td>jitter</td>
<td>Set jitter parameters for periodic interval</td>
</tr>
<tr>
<td>maximum</td>
<td>Set maximum jitter value for periodic interval (in seconds)</td>
</tr>
<tr>
<td>&lt;0-2147483&gt;</td>
<td>Maximum jitter value for periodic interval(in seconds). Default is 300 seconds.</td>
</tr>
</tbody>
</table>

### Command Default

None

### Command Modes

Global configuration (config)

### 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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1</td>
</tr>
</tbody>
</table>

### Examples

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

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# aaa accounting update periodic 5
```
aaa authentication dot1x

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

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

**Syntax Description**

- `default` The default method when a user logs in. Use the listed authentication method that follows this argument.
- `method1` Specifies the server authentication. Enter the `group radius` keywords to use the list of all RADIUS servers for authentication.

**Note** Though other keywords are visible in the command-line help strings, only the `default` and `group radius` keywords are supported.

**Command Default**

No authentication is performed.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

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

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

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

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

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

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

**Syntax Description**

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

**Command Default**

None

**Command Modes**

Global Configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

None

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

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

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

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

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

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

no aaa authorization { auth-proxy | cache | commands level | config-commands | configuration
| console | credential-download | exec | multicast | network | reverse-access | template}
{default | list_name} [method1 [ method2 . . . ]]
```

### Syntax Description

- **auth-proxy**
  - Runs authorization for authentication proxy services.

- **cache**
  - Configures the authentication, authorization, and accounting (AAA) server.

- **commands**
  - Runs authorization for all commands at the specified privilege level.

- **level**
  - Specific command level that should be authorized. Valid entries are 0 through 15.

- **config-commands**
  - Runs authorization to determine whether commands entered in configuration mode are authorized.

- **configuration**
  - Downloads the configuration from the AAA server.

- **console**
  - Enables the console authorization for the AAA server.

- **credential-download**
  - Downloads EAP credential from Local/RADIUS/LDAP.

- **exec**
  - Enables the console authorization for the AAA server.

- **multicast**
  - Downloads the multicast configuration from the AAA server.

- **network**
  - Runs authorization for all network-related service requests, including Serial Line Internet Protocol (SLIP), PPP, PPP Network Control Programs (NCPs), and AppleTalk Remote Access (ARA).

- **onep**
  - Runs authorization for the ONEP service.

- **reverse-access**
  - Runs authorization for reverse access connections, such as reverse Telnet.

- **template**
  - Enables template authorization for the AAA server.

- **default**
  - Uses the listed authorization methods that follow this keyword as the default list of methods for authorization.

- **list_name**
  - Character string used to name the list of authorization methods.
aaa authorization

(method1 [method2...]) (Optional) An authorization method or multiple authorization methods to be used for authorization. A method may be any one of the keywords listed in the table below.

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

**Command Modes**
Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

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

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

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

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

**Table 3: aaa authorization Methods**

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cache group-name</td>
<td>Uses a cache server group for authorization.</td>
</tr>
<tr>
<td>group group-name</td>
<td>Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the server group group-name command.</td>
</tr>
<tr>
<td>group ldap</td>
<td>Uses the list of all Lightweight Directory Access Protocol (LDAP) servers for authentication.</td>
</tr>
<tr>
<td>group radius</td>
<td>Uses the list of all RADIUS servers for authentication as defined by the aaa group server radius command.</td>
</tr>
<tr>
<td>group tacacs+</td>
<td>Uses the list of all TACACS+ servers for authentication as defined by the aaa group server tacacs+ command.</td>
</tr>
<tr>
<td>if-authenticated</td>
<td>Allows the user to access the requested function if the user is authenticated.</td>
</tr>
<tr>
<td>local</td>
<td>Uses the local database for authorization.</td>
</tr>
<tr>
<td>none</td>
<td>Indicates that no authorization is performed.</td>
</tr>
</tbody>
</table>

Cisco IOS software supports the following methods for authorization:

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

- **Commands**—Applies to the EXEC mode commands a user issues. Command authorization attempts authorization for all EXEC mode commands, including global configuration commands, associated with a specific privilege level.

- **EXEC**—Applies to the attributes associated with a user EXEC terminal session.

- **Network**—Applies to network connections. The network connections can include a PPP, SLIP, or ARA connection.

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

- **Reverse Access**—Applies to reverse Telnet sessions.

- **Configuration**—Applies to the configuration downloaded from the AAA server.

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

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

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

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

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

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

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

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

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

```
aaa authorization credential download default group-name
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>group-name</strong></td>
<td>Server group name.</td>
</tr>
</tbody>
</table>

**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 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

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

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

```
aaa group server ldap group-name
```

**Command Default**

None

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

This example shows how to configure a AAA server group:

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

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

```
aaa group server radius  group-name
```

**Syntax Description**

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

**Command Default**

None

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

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

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

```
Device(config)# aaa group server radius ISE_Group
```
## aaa local authentication default authorization

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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>method-list-name</code></td>
<td>Name of the method list.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>Global configuration (config)</td>
</tr>
<tr>
<td>Command History</td>
<td></td>
</tr>
</tbody>
</table>

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

### Examples

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

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

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

```
aaa new-model
no aaa new-model
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

AAA is not enabled.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command enables the AAA access control system.

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

---

**Note**

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

The following example shows this restriction:

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

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

**Examples**

The following example initializes AAA:

```
Device(config)# aaa new-model
Device(config)#
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa accounting</td>
<td>Enables AAA accounting of requested services for billing or security purposes.</td>
</tr>
<tr>
<td>aaa authentication arap</td>
<td>Enables an AAA authentication method for ARAP using TACACS+.</td>
</tr>
<tr>
<td>aaa authentication enable default</td>
<td>Enables AAA authentication to determine if a user can access the privileged command level.</td>
</tr>
<tr>
<td>aaa authentication login</td>
<td>Sets AAA authentication at login.</td>
</tr>
<tr>
<td>aaa authentication ppp</td>
<td>Specifies one or more AAA authentication method for use on serial interfaces running PPP.</td>
</tr>
<tr>
<td>aaa authorization</td>
<td>Sets parameters that restrict user access to a network.</td>
</tr>
</tbody>
</table>
aaa server radius dynamic-author

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

```plaintext
aaa server radius dynamic-author
no aaa server radius dynamic-author
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

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

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(28)SB</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.4</td>
<td>This command was integrated into Cisco IOS Release 12.4.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.6</td>
<td>This command was integrated into Cisco IOS XE Release 2.6.</td>
</tr>
<tr>
<td>12.2(5)SXI</td>
<td>This command was integrated into Cisco IOS Release 12.2(5)SXI.</td>
</tr>
<tr>
<td>15.2(2)T</td>
<td>This command was integrated into Cisco IOS Release 15.2(2)T.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Dynamic Authorization for the Intelligent Services Gateway (ISG)**

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

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

**Examples**

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

```plaintext
aaa server radius dynamic-author
client 10.12.12.12 key cisco
message-authenticator ignore
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth-type (ISG)</td>
<td>Specifies the server authorization type.</td>
</tr>
<tr>
<td>client</td>
<td>Specifies a RADIUS client from which a device will accept CoA and disconnect requests.</td>
</tr>
<tr>
<td>default</td>
<td>Sets a RADIUS application command to its default.</td>
</tr>
<tr>
<td>domain</td>
<td>Specifies username domain options.</td>
</tr>
<tr>
<td>ignore</td>
<td>Overrides a behavior to ignore certain parameters.</td>
</tr>
<tr>
<td>port</td>
<td>Specifies a port on which local RADIUS server listens.</td>
</tr>
<tr>
<td>server-key</td>
<td>Specifies the encryption key shared with RADIUS clients.</td>
</tr>
</tbody>
</table>
aaa session-id

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

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

**Syntax Description**

<table>
<thead>
<tr>
<th>common</th>
<th>(Optional) Ensures that all session identification (ID) information that is sent out for a given call will be made identical. The default behavior is <code>common</code>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>unique</td>
<td>(Optional) Ensures that only the corresponding service access-requests and accounting-requests will maintain a common session ID. Accounting-requests for each service will have a different session ID.</td>
</tr>
</tbody>
</table>

**Command Default**

The `common` keyword is enabled.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(4)B</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(8)T</td>
<td>This command was integrated into Cisco IOS Release 12.2(8)T.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

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

The `unique` keyword behavior assigns a different session ID for each accounting type (Auth-Proxy, Exec, Network, Command, System, Connection, and Resource) during a call. To specify this behavior, the `unique` keyword must be specified. The session ID may be included in RADIUS access requests by configuring the `radius-server attribute 44 include-in-access-req` command. The session ID in the access-request will be the
same as the session ID in the accounting request for the same service; all other services will provide unique session IDs for the same call.

**Examples**

The following example shows how to configure unique session IDs:

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa new model</td>
<td>Enables AAA.</td>
</tr>
<tr>
<td>radius-server attribute 44 include-in-access-req</td>
<td>Sends RADIUS attribute 44 (Accounting Session ID) in access request packets before user authentication (including requests for preauthentication).</td>
</tr>
</tbody>
</table>
aaa-override

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

```
AAA-override
no AAA-override
```

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

AAA is disabled by default.

**Command Modes**

WLAN configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

This example shows how to enable AAA on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# shutdown
Device(config-wlan)# aaa-override
Device(config-wlan)# no shutdown
Device(config-wlan)# end
```

This example shows how to disable AAA on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# shutdown
Device(config-wlan)# no aaa-override
Device(config-wlan)# no shutdown
Device(config-wlan)# end
```
aaa-policy

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

```
  aaa-policy  aaa-policy-name
```

**Syntax Description**

- `aaa-policy-name` Name of the AAA policy.

**Command Default**

None

**Command Modes**

config-wireless-policy

**Command History**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

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

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

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

### aaa-realm enable

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>config-aaa-policy</td>
</tr>
</tbody>
</table>

### 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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

### Examples

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

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless aaa policy aaa-profile-name
Device (config-aaa-policy)# aaa-realm enable
```
To enable an absolute timeout for subscriber sessions, use the `absolute-timer` command in service template configuration mode. To disable the timer, use the `no` form of this command.

```
absolute-timer minutes
no absolute-timer
```

**Syntax Description**

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

**Command Default**

Disabled (the absolute timeout is 0).

**Command Modes**

Service template configuration (config-service-template)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Examples**

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

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>event absolute-timeout</code></td>
<td>Specifies the type of event that triggers actions in a control policy if conditions are met.</td>
</tr>
<tr>
<td><code>inactivity-timer</code></td>
<td>Enables an inactivity timeout for subscriber sessions.</td>
</tr>
<tr>
<td><code>show service-template</code></td>
<td>Displays configuration information for service templates.</td>
</tr>
</tbody>
</table>
access-list

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

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

**Syntax Description**

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

**Command Default**

None

**Command Modes**

config

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to add an access list entry:
Device# `configure terminal`
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# `access-list 1 permit any`
access-list acl-ace-limit

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

```
access-list  acl-ace-limit  max-ace-limit
```

**Syntax Description**

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

**Command Default**

None

**Command Modes**

Global configuration (config)

**Command History**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

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

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

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

```
accounting-list  radius-server-acct
no accounting-list
```

**Syntax Description**

- `radius-server-acct` Accounting RADIUS server name.

**Command Default**
RADIUS server accounting is disabled by default.

**Command Modes**
WLAN policy configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

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

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

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

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

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

```
acl-policy acl-policy-name
```

**Syntax Description**
- acl-policy-name Name of the ACL policy.

**Command Default**
None

**Command Modes**
config-wireless-flex-profile

**Command History**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

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

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

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

```
address ip-address
no address ip-address
```

### Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address</td>
<td>IP address of the remote peer.</td>
</tr>
</tbody>
</table>

### Command Default

No default behavior or values

### Command Modes

Rsa-pubkey configuration

### Command History

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

### Usage Guidelines

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

### Examples

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

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

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto keyring</td>
<td>Defines a crypto keyring to be used during IKE authentication.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>key-string</td>
<td>Specifies the RSA public key of a remote peer.</td>
</tr>
<tr>
<td>rsa-pubkey</td>
<td>Defines the RSA manual key to be used for encryption or signatures during IKE authentication.</td>
</tr>
</tbody>
</table>
address prefix

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

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

**Syntax Description**

<table>
<thead>
<tr>
<th><code>ipv6-prefix</code></th>
<th>IPv6 address prefix.</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>lifetime</code></td>
<td>(Optional) Specifies a time interval (in seconds) that an IPv6 address prefix remains in the valid state. If the <code>infinite</code> keyword is specified, the time interval does not expire.</td>
</tr>
</tbody>
</table>

**Command Default**

No IPv6 address prefix is assigned.

**Command Modes**

DHCP pool configuration (config-dhcpv6)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(24)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Examples**

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

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6 dhcp pool</code></td>
<td>Configures a DHCPv6 server configuration information pool and enters DHCPv6 pool configuration mode.</td>
</tr>
</tbody>
</table>
airtime-fairness mode

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

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

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

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

**Command Default**
None

**Command Modes**
RF Profile configuration (config-rf-profile)

**Command History**
- Cisco IOS XE Gibraltar 16.10.1 This command was introduced.

This example shows how to configure air time fairness in different modes:
```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# ap dot11 24ghz rf-profile rfprof24_1
Device(config-rf-profile)# airtime-fairness mode enforce-policy
Device(config-rf-profile)# airtime-fairness optimization
Device(config-rf-profile)# end
```
allow at-least min-number at-most max-number

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

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

**Syntax Description**

- **at-least min-number**
  - Enter the minimum guaranteed number of multicast RAs per router before throttling can be enforced. Valid range is 0 to 32.

- **at-most max-number**
  - Enter the maximum number of multicast RAs from router by which throttling is enforced. Valid range is 0 to 256.

- **at-most no-limit**
  - No upper bound at the router level.

**Command Default**

None

**Command Modes**

config-nd-ra-throttle

**Command History**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

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

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

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

```plaintext
amsdu
```

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

`amsdu` is enabled.

**Command Modes**

`config-wireless-mesh-profile`

**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>

**Example**

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

```plaintext
Device # configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device (config)# wireless profile mesh mesh-profile
Device (config-wireless-mesh-profile)# amsdu
```
To configure cisco APs, use the `ap` command.

```
ap mac-address
```

**Syntax Description**

- `mac-address` Ethernet MAC address of the AP.

**Command Default**

None

**Command Modes**

- config

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

none.

**Example**

The following example shows how to configure a Cisco AP:

```
Device(config)# ap F866.F267.7DFB
```
ap auth-list ap-policy

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

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

### Syntax Description

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

### Command Default

None

### Command Modes

Global configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

This example shows how to enable the access point authorization policy:
```
Device(config)# ap auth-list ap-policy authorize-ap
```

This example shows how to enable access points with locally significant certificates to connect:
```
Device(config)# ap auth-list ap-policy lsc
```

This example shows how to enable access points with manufacture-installed certificates to connect:
```
Device(config)# ap auth-list ap-policy mic
```

This example shows how to enable access points with self-signed certificates to connect:
```
Device(config)# ap auth-list ap-policy ssc
```
ap auth-list ap-policy

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

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

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

**Command Default**
None

**Command Modes**
Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

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

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

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

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

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

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

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

To configure a primary or secondary backup device for all access points that are joined to a specific device, use the `ap capwap backup` command.

```
ap capwap backup {primary primary-controller-name primary-controller-ip-address | secondary secondary-controller-name secondary-controller-ip-address}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>primary</td>
<td>Specifies the primary backup device.</td>
</tr>
<tr>
<td>primary-controller-name</td>
<td>Primary backup device name.</td>
</tr>
<tr>
<td>primary-controller-ip-address</td>
<td>Primary backup device IP address.</td>
</tr>
<tr>
<td>secondary</td>
<td>Specifies the secondary backup device.</td>
</tr>
<tr>
<td>secondary-controller-name</td>
<td>Secondary backup device name.</td>
</tr>
<tr>
<td>secondary-controller-ip-address</td>
<td>Secondary backup device IP address.</td>
</tr>
</tbody>
</table>

**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 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

This example shows how to configure a primary backup device for all access points that are joined to a specific device:

```
Device(config)# ap capwap backup primary controller1 192.0.2.51
```

This example shows how to configure a secondary backup device for all access points that are joined to a specific device:

```
Device(config)# ap capwap backup secondary controller1 192.0.2.52
```
ap capwap multicast

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

```
ap capwap multicast {multicast-ip-address|service-policy output policymap-name}
```

**Syntax Description**

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

**Command Default**

None

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

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

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

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

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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>count retransmit-count</code></td>
<td>Specifies the access point CAPWAP control packet retransmit count.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The count is from 3 to 8 seconds.</td>
</tr>
<tr>
<td><code>interval retransmit-interval</code></td>
<td>Specifies the access point CAPWAP control packet retransmit interval.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The interval is from 2 to 5 seconds.</td>
</tr>
</tbody>
</table>

**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 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

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

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

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

To configure advanced timer settings, use the `ap capwap timers` command.

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>discovery-timeout</th>
<th>Specifies the Cisco lightweight access point discovery timeout.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Note</td>
<td>The Cisco lightweight access point discovery timeout is how long a Cisco device waits for an unresponsive access point to answer before considering that the access point failed to respond.</td>
</tr>
<tr>
<td></td>
<td>seconds</td>
<td>Cisco lightweight access point discovery timeout from 1 to 10 seconds.</td>
</tr>
<tr>
<td></td>
<td>Note</td>
<td>The default is 10 seconds.</td>
</tr>
<tr>
<td>fast-heartbeat-timeout local</td>
<td>seconds</td>
<td>Small heartbeat interval (from 1 to 10 seconds) that reduces the amount of time it takes to detect a device failure.</td>
</tr>
<tr>
<td>Note</td>
<td>The fast heartbeat time-out interval is disabled by default.</td>
<td></td>
</tr>
<tr>
<td>heartbeat-timeout</td>
<td>Specifies the Cisco lightweight access point heartbeat timeout.</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>The Cisco lightweight access point heartbeat timeout controls how often the Cisco lightweight access point sends a heartbeat keep-alive signal to the Cisco device.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This value should be at least three times larger than the fast heartbeat timer.</td>
<td></td>
</tr>
<tr>
<td>seconds</td>
<td>Cisco lightweight access point heartbeat timeout value from 1 to 30 seconds.</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>The default is 30 seconds.</td>
<td></td>
</tr>
<tr>
<td>primary-discovery-timeout</td>
<td>seconds</td>
<td>Specifies the access point primary discovery request timer. The timer determines the amount of time taken by an access point to discovery the configured primary, secondary, or tertiary device.</td>
</tr>
<tr>
<td>Note</td>
<td>The default is 120 seconds.</td>
<td></td>
</tr>
<tr>
<td>primed-join-timeout</td>
<td>Specifies the authentication timeout. Determines the time taken by an access point to determine that the primary device has become unresponsive. The access point makes no further attempts to join the device until the connection to the device is restored.</td>
<td></td>
</tr>
</tbody>
</table>
Authentication response timeout from 120 to 43200 seconds.

**Note**  The default is 120 seconds.

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>Global configuration</td>
</tr>
<tr>
<td>Command History</td>
<td>Release</td>
</tr>
<tr>
<td></td>
<td>Cisco IOS XE 3.2SE</td>
</tr>
</tbody>
</table>

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

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

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

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

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

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

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

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

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

```device(config)# ap capwap timers primed-join-timeout 360```
To enable the Cisco Discovery Protocol (CDP) on a Cisco lightweight access point, use the `ap cdp` command. To disable the Cisco Discovery Protocol (CDP) on a Cisco lightweight access point, use the `no` form of this command.

```plaintext
ap cdp [interface {ethernet ethernet-id|radio radio-id}]  
no ap cdp [interface {ethernet ethernet-id|radio radio-id}]  
```

### Syntax Description

- **interface** (Optional) Specifies CDP in a specific interface.
- **ethernet** Specifies CDP for an Ethernet interface.
- **ethernet-id** Ethernet interface number from 0 to 3.
- **radio** Specifies CDP for a radio interface.
- **radio-id** Radio number from 0 to 3.

### Command Default

Disabled on all access points.

### Command Modes

Global configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The `no ap cdp` command disables CDP on all access points that are joined to the device and all access points that join in the future. CDP remains disabled on both current and future access points even after the device or access point reboots. To enable CDP, enter the `ap cdp` command.

**Note**

CDP over Ethernet/radio interfaces is available only when CDP is enabled. After you enable CDP on all access points joined to the device, you can disable and then reenable CDP on individual access points using the `ap name Cisco-AP cdp` command. After you disable CDP on all access points joined to the device, you can enable and then disable CDP on individual access points.

This example shows how to enable CDP on all access points:

```plaintext
Device(config)# ap cdp  
```

This example shows how to enable CDP for Ethernet interface number 0 on all access points:

```plaintext
Device(config)# ap cdp ethernet 0  
```
To configure one or more country codes for a device, use the `ap country` command.

```
ap country country-code
```

**Syntax Description**

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

**Command Default**

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

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

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

```
Device(config)# ap country IN,FR
```
To configure Spectrum Intelligence (SI) on Qualcomm based 2.4 GHz or 5 GHz radios, use the `ap dot11 SI` command.

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

**Syntax Description**

- **24ghz** 2.4 GHz radio
- **5ghz** 5 GHz radio
- **SI** Enable Spectrum Intelligence (SI). `[no]` in the command disables SI.

**Command Default**

None

**Command Modes**

Global configuration (config)

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

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

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# ap dot11 5ghz SI
```
**ap dot11 24ghz cleanair**

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

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

**Command Default**
Disabled.

**Command Modes**
Global configuration (config).

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

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

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

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

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

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ble-beacon</td>
<td>Configure the BLE beacon feature.</td>
</tr>
<tr>
<td>bt-discovery</td>
<td>Configures the alarm for Bluetooth interference devices.</td>
</tr>
<tr>
<td>bt-link</td>
<td>Configures the alarm for any Bluetooth link.</td>
</tr>
<tr>
<td>canopy</td>
<td>Configures the alarm for canopy interference devices.</td>
</tr>
<tr>
<td>cont-tx</td>
<td>Configures the alarm for continuous transmitters.</td>
</tr>
<tr>
<td>dect-like</td>
<td>Configures the alarm for Digital Enhanced Cordless Communication (DECT)-like phones.</td>
</tr>
<tr>
<td>fh</td>
<td>Configures the alarm for 802.11 frequency hopping devices.</td>
</tr>
<tr>
<td>inv</td>
<td>Configures the alarm for devices using spectrally inverted Wi-Fi signals.</td>
</tr>
<tr>
<td>jammer</td>
<td>Configures the alarm for jammer interference devices.</td>
</tr>
<tr>
<td>mw-oven</td>
<td>Configures the alarm for microwave ovens.</td>
</tr>
<tr>
<td>nonstd</td>
<td>Configures the alarm for devices using nonstandard Wi-Fi channels.</td>
</tr>
<tr>
<td>superag</td>
<td>Configures the alarm for 802.11 SuperAG interference devices.</td>
</tr>
<tr>
<td>tdd-tx</td>
<td>Configures the alarm for Time Division Duplex (TDD) transmitters.</td>
</tr>
<tr>
<td>video</td>
<td>Configures the alarm for video cameras.</td>
</tr>
<tr>
<td>Command Default</td>
<td>The alarm for Wi-Fi inverted devices is enabled. The alarm for all other devices is disabled.</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Command Modes</td>
<td>Global configuration (config).</td>
</tr>
<tr>
<td>Command History</td>
<td><strong>Release</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Release</strong></td>
</tr>
<tr>
<td>Usage Guidelines</td>
<td>You must enable CleanAir using the <strong>ap dot11 24ghz cleanair</strong> command before you configure this command.</td>
</tr>
<tr>
<td></td>
<td>This example shows how to enable CleanAir to report when a video camera interferes:</td>
</tr>
<tr>
<td></td>
<td><strong>Device(config)# default ap dot11 24ghz cleanair device video</strong></td>
</tr>
</tbody>
</table>
ap dot11 24ghz dot11g

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

```
ap dot11 24ghz dot11g
no ap dot11 24ghz dot11g
```

**Syntax Description**

This command has no keywords and arguments.

**Command Default**

Enabled

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

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

This example shows how to enable the 802.11g network:

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

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

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

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

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>Global configuration (config)</td>
</tr>
<tr>
<td>Command History</td>
<td>Release   Modification</td>
</tr>
<tr>
<td></td>
<td>Cisco IOS XE Gibraltar 16.10.1  This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>
Examples

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

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

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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>data-rate-threshold</th>
<th>Configure the data rate threshold for 802.11b optimized roaming.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>11M</td>
<td>Sets the data rate threshold for 802.11b optimized roaming to 11 Mbps</td>
</tr>
<tr>
<td>12M</td>
<td>Sets the data rate threshold for 802.11b optimized roaming to 12 Mbps</td>
</tr>
<tr>
<td>18M</td>
<td>Sets the data rate threshold for 802.11b optimized roaming to 18 Mbps</td>
</tr>
<tr>
<td>1M</td>
<td>Sets the data rate threshold for 802.11b optimized roaming to 1 Mbps</td>
</tr>
<tr>
<td>24M</td>
<td>Sets the data rate threshold for 802.11b optimized roaming to 24 Mbps</td>
</tr>
<tr>
<td>2M</td>
<td>Sets the data rate threshold for 802.11b optimized roaming to 2 Mbps</td>
</tr>
<tr>
<td>36M</td>
<td>Sets the data rate threshold for 802.11b optimized roaming to 36 Mbps</td>
</tr>
<tr>
<td>48M</td>
<td>Sets the data rate threshold for 802.11b optimized roaming to 48 Mbps</td>
</tr>
<tr>
<td>54M</td>
<td>Sets the data rate threshold for 802.11b optimized roaming to 54 Mbps</td>
</tr>
<tr>
<td>5_5M</td>
<td>Sets the data rate threshold for 802.11b optimized roaming to 5.5 Mbps</td>
</tr>
<tr>
<td>6M</td>
<td>Sets the data rate threshold for 802.11b optimized roaming to 6 Mbps</td>
</tr>
<tr>
<td>9M</td>
<td>Sets the data rate threshold for 802.11b optimized roaming to 9 Mbps</td>
</tr>
<tr>
<td>disable</td>
<td>Disables the data rate threshold.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

Global configuration (config)

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

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

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

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

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

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>24ghz</td>
<td>Specifies the 2.4 GHz band.</td>
</tr>
<tr>
<td>5ghz</td>
<td>Specifies the 5 GHz band.</td>
</tr>
<tr>
<td>sensitivity</td>
<td>Sets the sensitivity for CleanAir event-driven RRM.</td>
</tr>
<tr>
<td>value</td>
<td>Sensitivity value. You can specify any one of the following three optional sensitivity values:</td>
</tr>
<tr>
<td></td>
<td>• low—Specifies low sensitivity.</td>
</tr>
<tr>
<td></td>
<td>• medium—Specifies medium sensitivity.</td>
</tr>
<tr>
<td></td>
<td>• high—Specifies high sensitivity.</td>
</tr>
</tbody>
</table>

**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 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

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

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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>sensitivity</td>
<td>(Optional) Configures the EDRRM sensitivity of the CleanAir event.</td>
</tr>
<tr>
<td>high</td>
<td>(Optional) Specifies the highest sensitivity to non-Wi–Fi interference as indicated by the air quality (AQ) value.</td>
</tr>
<tr>
<td>low</td>
<td>(Optional) Specifies the least sensitivity to non-Wi–Fi interference as indicated by the AQ value.</td>
</tr>
<tr>
<td>medium</td>
<td>(Optional) Specifies medium sensitivity to non-Wi–Fi interference as indicated by the AQ value.</td>
</tr>
</tbody>
</table>

**Command Default**
EDRRM is disabled and the sensitivity is low.

**Command Modes**
Global configuration (config).

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

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

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

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

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

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

**Command Default**
Persistent device avoidance is disabled.

**Command Modes**
Global configuration (config).

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

This example shows how to enable persistent device avoidance:

```
Device(config)# ap dot11 24ghz rrm channel device
```
ap dot11 24ghz rx-sop threshold

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

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

**Syntax Description**

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

**Command Default**

None

**Command Modes**

Global configuration (config)

**Command History**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Table 4: RxSOP Thresholds for 2.4-GHz Band**

<table>
<thead>
<tr>
<th>High Threshold</th>
<th>Medium Threshold</th>
<th>Low Threshold</th>
<th>Custom Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>–79 dBm</td>
<td>–82 dBm</td>
<td>–85 dBm</td>
<td>–85 dBm to –60 dBm</td>
</tr>
</tbody>
</table>

**Examples**

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

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# ap dot11 24ghz rx-sop threshold auto
```
ap dot11 5ghz channelswitch mode

To configure a 802.11h channel switch announcement, use the `ap dot11 5ghz channelswitch mode` command. To disable a 802.11h channel switch announcement, use the `no ap dot11 5ghz channelswitch mode` command.

```
ap dot11 5ghz channelswitch mode value
no ap dot11 5ghz channelswitch mode
```

**Syntax Description**

- `value` 802.11h channel announcement value.

**Note**
You can specify anyone of the following two values:

- 0—Indicates that the channel switch announcement is disabled.
- 1—Indicates that the channel switch announcement is enabled.

---

**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 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

This example shows how to enable the 802.11h switch announcement:

```
Device(config)# ap dot11 5ghz channelswitch mode 1
```
ap dot11 5ghz channelswitch quiet

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

**Command Default**

None

**Command Modes**

Global configuration (config)

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

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

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

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

**Command Default**

Disabled.

**Command Modes**

Global configuration.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

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

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

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

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

**Syntax Description**

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

**Command Default**

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

**Command Modes**

Global configuration (config).

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

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

```
Device(config)# default ap dot11 5ghz cleanair device video
```
ap dot11 5ghz dot11ac frame-burst automatic

To configure a 802.11ac frame-burst, use the `ap dot11 5ghz dot11ac frame-burst automatic` command. To disable a 802.11ac frame-burst, use the `no` form of this command.

```
ap dot11 5ghz dot11ac frame-burst automatic
no ap dot11 5ghz dot11ac frame-burst automatic
```

**Syntax Description**

This command has no keywords and 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 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Before you enter the `ap dot11 5ghz dot11ac frame-burst automatic` command, disable the 802.11 Cisco radio with the `ap dot11 5ghz shutdown` command.

**Example**

This example shows how to enable 802.11ac frame-burst

```
Device(config)# ap dot11 5ghz dot11ac frame-burst automatic
```
ap dot11 5ghz power-constraint

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

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

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>802.11h power constraint value.</td>
</tr>
</tbody>
</table>

**Note**
The range is from 0 to 30 dBm.

**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 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

```
Device(config)# ap dot11 5ghz power-constraint 5
```
To configure 802.11a operational rates, use the `ap dot11 5ghz rate` command.

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

### Syntax Description

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

### Command Default

None

### Command Modes

Global configuration (config)

### Command History

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

### Examples

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

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# ap dot11 5ghz rate RATE_24M supported
```
To enable Event-Driven RRM (EDRRM) and configure the sensitivity for 5-GHz devices, use the `ap dot11 5ghz rrm channel cleanair-event` command in global configuration mode. To disable EDRRM, use the `no` form of the command.

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

**Syntax Description**

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

**Command Default**

EDRRM is disabled and the EDRRM sensitivity is low.

**Command Modes**

Global configuration (config).

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

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

```bash
Device(config)# ap dot11 5ghz rrm channel cleanair-event  
Device(config)# ap dot11 5ghz rrm channel cleanair-event sensitivity high
```
To configure persistent non-Wi-Fi device avoidance in the 802.11a channel, use the `ap dot11 5ghz rrm channel device` command in global configuration mode. To disable persistent device avoidance, use the `no` form of this command.

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

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

**Command Default**
The CleanAir persistent device state is disabled.

**Command Modes**
Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

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

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

To configure a 802.11h channel switch announcement, use the `ap dot11 5ghz channelswitch mode` command. To disable a 802.11h channel switch announcement, use the `no` form of this command.

```plaintext
ap dot11 5ghz channelswitch mode value
no ap dot11 5ghz channelswitch mode
```

**Syntax Description**

<table>
<thead>
<tr>
<th><strong>value</strong></th>
<th>802.11h channel announcement value.</th>
</tr>
</thead>
</table>

**Note**

You can specify any one of the following two values:

- 0—Indicates that the channel switch announcement is disabled.
- 1—Indicates that the channel switch announcement is enabled.

**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 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

This example shows how to enable the 802.11h switch announcement:

```plaintext
Device(config)# ap dot11 5ghz channelswitch mode 1
```
ap dot11 5ghz rx-sop threshold

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

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

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto</td>
<td>Reverts RxSOP value to the default value.</td>
</tr>
<tr>
<td>high</td>
<td>Sets the RxSOP value to high threshold (–76 dBm).</td>
</tr>
<tr>
<td>medium</td>
<td>Sets the RxSOP value to medium threshold (–78 dBm).</td>
</tr>
<tr>
<td>low</td>
<td>Sets the RxSOP value to low threshold (–80 dBm).</td>
</tr>
<tr>
<td>custom</td>
<td>Sets the RxSOP value to custom threshold (–85 dBm to –60 dBm)</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

`config`

**Command History**

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

**Usage Guidelines**

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

**Table 5: RxSOP Thresholds for 5-GHz Band**

<table>
<thead>
<tr>
<th>High Threshold</th>
<th>Medium Threshold</th>
<th>Low Threshold</th>
<th>Custom Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>–76 dBm</td>
<td>–78 dBm</td>
<td>–80 dBm</td>
<td>–85 dBm to –60 dBm</td>
</tr>
</tbody>
</table>

**Examples**

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

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# ap dot11 24ghz rx-sop threshold custom –70
```
ap dot11 5ghz shutdown

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

**ap dot11 5ghz shutdown**

**Command Default**

None

**Command Modes**

Global configuration (config)

**Command History**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

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

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

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

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>config</td>
</tr>
<tr>
<td>Command History</td>
<td></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.

Examples

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

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

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

---

**Note**

Disable the 802.11 network before using this command. See the “Usage Guidelines” section.

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

**Syntax Description**

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

**Command Default**

None

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

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

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

```
Device(config) # ap dot11 5ghz beaconperiod 120
```
**ap dot11 cac media-stream**

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

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

<table>
<thead>
<tr>
<th><strong>Syntax Description</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>24ghz</code></td>
<td>Specifies the 2.4 GHz band.</td>
</tr>
<tr>
<td><code>5ghz</code></td>
<td>Specifies the 5 GHz band.</td>
</tr>
<tr>
<td><code>multicast-direct</code></td>
<td>Specifies CAC parameters for multicast-direct media streams.</td>
</tr>
<tr>
<td><code>max-retry-percent</code></td>
<td>Specifies the percentage of maximum retries that are allowed for multicast-direct media streams.</td>
</tr>
<tr>
<td><code>retryPercent</code></td>
<td>Percentage of maximum retries that are allowed for multicast-direct media streams.</td>
</tr>
<tr>
<td><code>min-client-rate</code></td>
<td>Specifies the minimum transmission data rate to the client for multicast-direct media streams (rate at which the client must transmit in order to receive multicast-direct unicast streams).</td>
</tr>
</tbody>
</table>

**Note**

If the transmission rate is below this rate, either the video will not start or the client may be classified as a bad client. The bad client video can be demoted for better effort QoS or subject to denial.
You can choose the following rates:

- eighteen
- eleven
- fiftyFour
- fivePointFive
- fortyEight
- nine
- one
- oneFifty
- oneFortyFourPointFour
- oneThirty
- oneThirtyFive
- seventyTwoPointTwo
- six
- sixtyFive
- thirtySix
- threeHundred
- twelve
- twentyFour
- two
- twoSeventy

**Command Default**

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

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

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

- Disable all WLANs with WMM enabled by entering the `wlan wlan_name shutdown` command.
• Disable the radio network you want to configure by entering the `ap dot11 {24ghz | 5ghz} shutdown` command.

• Save the new configuration.

• Enable voice or video CAC for the network you want to configure by entering the `ap dot11 {24ghz | 5ghz} cac voice acm` or `ap dot11 {24ghz | 5ghz} cac video acm` commands.

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

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

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

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

**Syntax Description**

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

**Command Default**

The default value is 75%.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

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

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

- Disable the radio network you want to configure by entering the `ap dot11 {24ghz | 5ghz} shutdown` command.

- Save the new configuration.

- Enable voice or video CAC for the network you want to configure by entering the `ap dot11 {24ghz | 5ghz} cac voice acm` or `ap dot11 {24ghz | 5ghz} cac video acm` commands.

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

```
Device(config)# ap dot11 5ghz cac multimedia max-bandwidth 5
```
To configure Call Admission Control (CAC) parameters for the video category, use the `ap dot11 cac video` command. To disable the CAC parameters for video category, use the `no` form of this command.

```
ap dot11 {24ghz|5ghz} cac video {acm|max-bandwidth value|roam-bandwidth value}
no ap dot11 {24ghz|5ghz} cac video {acm|max-bandwidth value|roam-bandwidth value}
```

### Syntax Description

- **24ghz**: Specifies the 2.4 GHz band.
- **5ghz**: Specifies the 5 GHz band.
- **acm**: Enables bandwidth-based video CAC for the 2.4 GHz or 5 GHz band.
  - **Note**: To disable bandwidth-based video CAC for the 2.4 GHz or 5 GHz band, use the `no ap dot11 {24ghz | 5ghz} cac video acm` command.
- **max-bandwidth**: Sets the percentage of the maximum bandwidth allocated to clients for video applications on the 2.4 GHz or 5 GHz band.
- **value**: Bandwidth percentage value from 5 to 85%.
- **roam-bandwidth**: Sets the percentage of the CAC maximum allocated bandwidth reserved for roaming video clients on the 2.4 GHz or 5 GHz band.
- **value**: Bandwidth percentage value from 0 to 85%.

### 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 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

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

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

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

This example shows how to enable the bandwidth-based CAC:
Device(config)# ap dot11 24ghz cac video acm

This example shows how to specify the percentage of the maximum allocated bandwidth for video applications on the selected radio band:
Device(config)# ap dot11 24ghz cac video max-bandwidth 50

This example shows how to configure the percentage of the maximum allocated bandwidth reserved for roaming video clients on the selected radio band:
Device(config)# ap dot11 24ghz cac video roam-bandwidth 10
### ap dot11 cac voice

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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>24ghz</th>
<th>Specifies the 2.4 GHz band.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>5ghz</td>
<td>Specifies the 5 GHz band.</td>
</tr>
<tr>
<td><strong>acm</strong></td>
<td></td>
<td>Enables bandwidth-based voice CAC for the 2.4 GHz or 5 GHz band.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td></td>
<td>To disable bandwidth-based voice CAC for the 2.4 GHz or 5 GHz band, use the **no ap dot11 {24ghz</td>
</tr>
</tbody>
</table>

- **load-based**: Enable load-based CAC on voice access category.  
  - **Note**: To disable load-based CAC on voice access category for the 2.4 GHz or 5 GHz band, use the **no ap dot11 {24ghz | 5ghz} cac voice load-based** command.

- **max-bandwidth**: Sets the percentage of the maximum bandwidth allocated to clients for voice applications on the 2.4 GHz or 5 GHz band.
  - **value**: Bandwidth percentage value from 5 to 85%.

- **roam-bandwidth**: Sets the percentage of the CAC maximum allocated bandwidth reserved for roaming voice clients on the 2.4 GHz or 5 GHz band.
  - **value**: Bandwidth percentage value from 0 to 85%.

- **sip**: Specifies the CAC codec name and sample interval as parameters and calculates the required bandwidth per call for the 802.11 networks.

- **bandwidth**: (Optional) Specifies bandwidth for a SIP-based call.
**bw**

Bandwidth in kbps. The following bandwidth values specify parameters for the SIP codecs:

- **64kbps**—Specifies CAC parameters for the SIP G711 codec.
- **8kbps**—Specifies CAC parameters for the SIP G729 codec.

**Note**  The default value is 64 Kbps.

**sample-interval**

Specifies the packetization interval for SIP codec.

**value**

Packetization interval in msecs. The sample interval for SIP codec value is 20 seconds.

**stream-size**

Specifies the number of aggregated voice Wi-Fi Multimedia (WMM) traffic specification (TSPEC) streams at a specified data rate for the 2.4 GHz or 5 GHz band.

**x**

Stream size. The range of the stream size is from 84000 to 92100.

**max-streams**

Specifies the maximum number of streams per TSPEC.

**y**

Number (1 to 5) of voice streams.

**Note**  The default number of streams is 2 and the mean data rate of a stream is 84 kbps.

**tspec-inactivity-timeout**

Specifies TSPEC inactivity timeout processing mode.

**Note**  Use this keyword to process or ignore the Wi-Fi Multimedia (WMM) traffic specifications (TSPEC) inactivity timeout received from an access point. When the inactivity timeout is ignored, a client TSPEC is not deleted even if the access point reports an inactivity timeout for that client.

**enable**

Processes the TSPEC inactivity timeout messages.

**ignore**

Ignores the TSPEC inactivity timeout messages.

**Note**  The default is ignore (disabled).

---

**Command Default**  None

**Command Modes**  Global configuration
### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>24ghz</td>
<td>Specifies the 2.4 GHz band.</td>
</tr>
<tr>
<td>5ghz</td>
<td>Specifies the 5 GHz band.</td>
</tr>
<tr>
<td>cleanair</td>
<td>Specifies CleanAir on the 2.4 GHz or 5 GHz band.</td>
</tr>
</tbody>
</table>

**Command Default**

Disabled

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

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

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

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

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>all</code></td>
<td>Specifies all device types.</td>
</tr>
<tr>
<td><code>device</code></td>
<td>Specifies the CleanAir interference device type.</td>
</tr>
<tr>
<td><code>bt-discovery</code></td>
<td>Specifies the Bluetooth device in discovery mode.</td>
</tr>
<tr>
<td><code>bt-link</code></td>
<td>Specifies the Bluetooth active link.</td>
</tr>
<tr>
<td><code>canopy</code></td>
<td>Specifies the Canopy devices.</td>
</tr>
<tr>
<td><code>cont-tx</code></td>
<td>Specifies the continuous transmitter.</td>
</tr>
<tr>
<td><code>dect-like</code></td>
<td>Specifies a Digital Enhanced Cordless Communication (DECT)-like phone.</td>
</tr>
<tr>
<td><code>fh</code></td>
<td>Specifies the 802.11 frequency hopping devices.</td>
</tr>
<tr>
<td><code>inv</code></td>
<td>Specifies the devices using spectrally inverted Wi-Fi signals.</td>
</tr>
<tr>
<td><code>jammer</code></td>
<td>Specifies the jammer.</td>
</tr>
<tr>
<td><code>mw-oven</code></td>
<td>Specifies the microwave oven devices.</td>
</tr>
<tr>
<td><code>nonstd</code></td>
<td>Specifies the devices using nonstandard Wi-Fi channels.</td>
</tr>
<tr>
<td><code>superag</code></td>
<td>Specifies 802.11 SuperAG devices.</td>
</tr>
<tr>
<td><code>tdd-tx</code></td>
<td>Specifies the TDD transmitter.</td>
</tr>
<tr>
<td><code>video</code></td>
<td>Specifies video cameras.</td>
</tr>
<tr>
<td><code>wimax-fixed</code></td>
<td>Specifies a WiMax fixed device.</td>
</tr>
<tr>
<td><code>wimax-mobile</code></td>
<td>Specifies a WiMax mobile device.</td>
</tr>
<tr>
<td><code>xbox</code></td>
<td>Specifies the Xbox device.</td>
</tr>
<tr>
<td><code>zigbee</code></td>
<td>Specifies the ZigBee device.</td>
</tr>
</tbody>
</table>

### 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 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

```
Device(config)# ap dot11 24ghz cleanair device zigbee
```
### ap dot11 dot11n

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

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

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

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

### Command Default

By default, priority 0 is enabled.

### Command Modes

Global configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE 3.3SE</td>
<td>The scheduler, timeout, and rt keywords were added.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

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

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

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

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

**Note**

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

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

Device(config)# ap dot11 24ghz dot11n

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

Device(config)# ap dot11 24ghz dot11n a-msdu tx priority all
This example shows how to enable only long guard intervals:

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

This example shows how to specify MCS rates:

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

This example shows how to enable RIFS:

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

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

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

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>24ghz</td>
<td>Specifies the 2.4 GHz band.</td>
</tr>
<tr>
<td>5ghz</td>
<td>Specifies the 5 GHz band.</td>
</tr>
</tbody>
</table>
| dtpc | Specifies Dynamic Transport Power Control (DTPC) settings.  

**Note** This option is enabled by default.

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
</table>
| exp-bwreq | Specifies Cisco Client eXtension (CCX) version 5 expedited bandwidth request feature.  

**Note** The expedited bandwidth request feature is disabled by default.

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
</table>
| fragmentation threshold | Specifies the fragmentation threshold.  

**Note** This option can only used be when the network is disabled using the `ap dot11 {24ghz|5ghz} shutdown` command.

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>threshold</td>
<td>Threshold. The range is from 256 to 2346 bytes (inclusive).</td>
</tr>
</tbody>
</table>

**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 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

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

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

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

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

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

```
Device(config)# ap dot11 5ghz fragmentation threshold 1500
```
Device(config)# ap dot11 5ghz fragmentation 1500
ap dot11 edca-parameters

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

```
ap dot11 {24ghz|5ghz} edca-parameters {custom-voice|optimized-video-voice|optimized-voice|svp-voice|wmm-default}
no ap dot11 {24ghz|5ghz} edca-parameters {custom-voice|optimized-video-voice|optimized-voice|svp-voice|wmm-default}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>24ghz</code></td>
<td>Specifies the 2.4 GHz band.</td>
</tr>
<tr>
<td><code>5ghz</code></td>
<td>Specifies the 5 GHz band.</td>
</tr>
<tr>
<td><code>edca-parameters</code></td>
<td>Specifies a specific enhanced distributed channel access (EDCA) profile on the 802.11 networks.</td>
</tr>
<tr>
<td><code>custom-voice</code></td>
<td>Enables custom voice EDCA parameters.</td>
</tr>
<tr>
<td><code>optimized-video-voice</code></td>
<td>Enables EDCA voice- and video-optimized profile parameters. Choose this option when both voice and video services are deployed on your network.</td>
</tr>
<tr>
<td><code>optimized-voice</code></td>
<td>Enables EDCA voice-optimized profile parameters. Choose this option when voice services other than SpectraLink are deployed on your network.</td>
</tr>
<tr>
<td><code>svp-voice</code></td>
<td>Enables SpectraLink voice priority parameters. Choose this option if SpectraLink phones are deployed on your network to improve the quality of calls.</td>
</tr>
<tr>
<td><code>wmm-default</code></td>
<td>Enables the Wi-Fi Multimedia (WMM) default parameters. Choose this option when voice or video services are not deployed on your network.</td>
</tr>
</tbody>
</table>

### Command Default

`wmm-default`

### Command Modes

Global configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>10.3</td>
<td>The <code>custom-voice</code> keyword was removed for Cisco 5700 Series WLC.</td>
</tr>
</tbody>
</table>

This example shows how to enable SpectraLink voice priority parameters:

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

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

```
ap dot11 {24GHz | 5GHz} rf-profile profile name
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>24ghz</td>
<td>Displays the 2.4-GHz band</td>
</tr>
<tr>
<td>5ghz</td>
<td>Displays the 5-GHz band</td>
</tr>
<tr>
<td>profile name</td>
<td>Name of the RF profile</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Denali 16.3.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

None

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

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

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

```
ap dot11 {24GHz | 5GHz} rf-profile profile name
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>24ghz</th>
<th>Displays the 2.4-GHz band</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>5ghz</td>
<td>Displays the 5-GHz band</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>profile name</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Denali 16.3.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

None

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

```
Device#ap dot11 24GHz rf-profile doctest
```
To configure basic and advanced radio resource management settings for 802.11 devices, use the **ap dot11 rrm** command.

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

<table>
<thead>
<tr>
<th><strong>Syntax Description</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>ccx</td>
<td>Configures Advanced (RRM) 802.11 CCX options.</td>
</tr>
<tr>
<td>location-measurement</td>
<td>Specifies 802.11 CCX Client Location Measurements in seconds. The range is between 10 and 32400 seconds.</td>
</tr>
<tr>
<td>channel</td>
<td>Configure advanced 802.11-channel assignment parameters.</td>
</tr>
<tr>
<td>cleanair-event</td>
<td>Configures cleanair event-driven RRM parameters.</td>
</tr>
<tr>
<td>dca</td>
<td>Configures 802.11-dynamic channel assignment algorithm parameters.</td>
</tr>
<tr>
<td>device</td>
<td>Configures persistent non-WiFi device avoidance in the 802.11-channel assignment.</td>
</tr>
<tr>
<td>foreign</td>
<td>Enables foreign AP 802.11-interference avoidance in the channel assignment.</td>
</tr>
<tr>
<td>load</td>
<td>Enables Cisco AP 802.11-load avoidance in the channel assignment.</td>
</tr>
<tr>
<td>noise</td>
<td>Enables non-802.11-noise avoidance in the channel assignment.</td>
</tr>
<tr>
<td>outdoor-ap-dca</td>
<td>Configures 802.11 DCA list option for outdoor AP.</td>
</tr>
<tr>
<td>coverage</td>
<td>Configures 802.11 coverage Hole-Detection.</td>
</tr>
<tr>
<td>Command</td>
<td>Default</td>
</tr>
<tr>
<td>------------------</td>
<td>------------</td>
</tr>
<tr>
<td><strong>data fail-percentage</strong> pct</td>
<td>Configures 802.11 coverage failure-rate threshold for uplink data packets. The range is between 1 and 100.</td>
</tr>
<tr>
<td><strong>data packet-count</strong> count</td>
<td>Configures 802.11 coverage minimum-failure-count threshold for uplink data packets.</td>
</tr>
<tr>
<td><strong>data rssi-threshold</strong> threshold</td>
<td>Configures 802.11 minimum-receive-coverage level for voice packets.</td>
</tr>
<tr>
<td><strong>exception global</strong> percentage</td>
<td>Configures 802.11 Cisco APs coverage-exception level. The range is between 0 and 100 percent.</td>
</tr>
<tr>
<td><strong>level global</strong> number</td>
<td>Configures 802.11 Cisco AP client-minimum-exception level between 1 and 75 clients.</td>
</tr>
<tr>
<td><strong>voice</strong></td>
<td>Configures 802.11 coverage Hole-Detection for voice packets.</td>
</tr>
<tr>
<td><strong>fail-percentage</strong> percentage</td>
<td>Configures 802.11 coverage failure rate threshold for uplink voice packets.</td>
</tr>
<tr>
<td><strong>packet-count</strong> number</td>
<td>Configures 802.11 coverage minimum-uplink-failure count threshold for voice packets.</td>
</tr>
<tr>
<td><strong>rssi-threshold</strong> threshold</td>
<td>Configures 802.11 minimum receive coverage level for voice packets.</td>
</tr>
</tbody>
</table>

**Command Default**

- Disabled

**Command Modes**

- Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

This example shows how to configure various RRM settings.

```
Device#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)#ap dot11 5ghz rrm ?
```
ccx                  Configure Advanced(RRM) 802.11a CCX options
channel             Configure advanced 802.11a channel assignment parameters
coverage            802.11a Coverage Hole Detection
group-member        Configure members in 802.11a static RF group
group-mode          802.11a RF group selection mode
logging             802.11a event logging
monitor             802.11a statistics monitoring
ndp-type             Neighbor discovery type Protected/Transparent
profile             802.11a performance profile
tpc-threshold       Configures the Tx Power Control Threshold used by RRM for auto
                    power assignment
txpower              Configures the 802.11a Tx Power Level
**ap dot11 rrm channel**

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

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

### Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cleanair-event</td>
<td>Specifies the cleanair event-driven RRM parameters</td>
</tr>
<tr>
<td>dca</td>
<td>Specifies the 802.11 dynamic channel assignment algorithm parameters</td>
</tr>
<tr>
<td>device</td>
<td>Specifies the persistent non-WiFi device avoidance in the 802.11-channel assignment.</td>
</tr>
<tr>
<td>foreign</td>
<td>Enables foreign AP 802.11-interference avoidance in the channel assignment.</td>
</tr>
<tr>
<td>load</td>
<td>Enables Cisco AP 802.11-load avoidance in the channel assignment.</td>
</tr>
<tr>
<td>noise</td>
<td>Enables non-802.11-noise avoidance in the channel assignment.</td>
</tr>
</tbody>
</table>

### Command Default

None.

### Command Modes

Interface configuration.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

None.

This example shows all the parameters available for Channel.

```
Device(config)#ap dot11 24ghz rrm channel ?
cleanair-event Configure cleanair event-driven RRM parameters
dca Config 802.11b dynamic channel assignment algorithm parameters
device Configure persistent non-WiFi device avoidance in the 802.11b channel assignment
foreign Configure foreign AP 802.11b interference avoidance in the channel assignment
load Configure Cisco AP 802.11b load avoidance in the channel assignment
noise Configure 802.11b noise avoidance in the channel assignment
```
# ap dot11 rrm channel dca

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

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

## Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>24ghz</code></td>
<td>Specifies the 2.4 GHz band.</td>
</tr>
<tr>
<td><code>5ghz</code></td>
<td>Specifies the 5 GHz band.</td>
</tr>
<tr>
<td><code>channel_number</code></td>
<td>Channel number to be added to the DCA list.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The range is from 1 to 14.</td>
</tr>
<tr>
<td><code>anchor-time value</code></td>
<td>Specifies the anchor time for DCA.</td>
</tr>
<tr>
<td><code>global</code></td>
<td>Specifies the global DCA mode for the access points in the 802.11 networks.</td>
</tr>
<tr>
<td><code>auto</code></td>
<td>Enables auto-RF.</td>
</tr>
<tr>
<td><code>once</code></td>
<td>Enables one-time auto-RF.</td>
</tr>
<tr>
<td><code>interval value</code></td>
<td>Specifies how often the DCA is allowed to run.</td>
</tr>
<tr>
<td><code>min-metric value</code></td>
<td>Specifies the DCA minimum RSSI energy metric.</td>
</tr>
<tr>
<td>`sensitivity {high</td>
<td>low</td>
</tr>
</tbody>
</table>

## Command Default

None

## Command Modes

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

To aid in troubleshooting, the output of this command shows an error code for any failed calls. The table below explains the possible error codes for failed calls.

**Table 6: DCA Sensitivity Threshold**

<table>
<thead>
<tr>
<th>Sensitivity</th>
<th>2.4 GHz DCA Sensitivity Threshold</th>
<th>5 GHz DCA Sensitivity Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>5 dB</td>
<td>5 dB</td>
</tr>
<tr>
<td>Medium</td>
<td>15 dB</td>
<td>20 dB</td>
</tr>
<tr>
<td>Low</td>
<td>30 dB</td>
<td>35 dB</td>
</tr>
</tbody>
</table>

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

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

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

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

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

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

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

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

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>data</code></td>
<td>Specifies 802.11 coverage hole-detection data packets.</td>
</tr>
<tr>
<td><code>fail-percentage</code></td>
<td>Specifies 802.11 coverage failure-rate threshold for uplink data packets.</td>
</tr>
<tr>
<td><code>percentage</code></td>
<td>The range is between 1 and 100.</td>
</tr>
<tr>
<td><code>packet-count</code></td>
<td>Specifies 802.11 coverage minimum-failure-count threshold for uplink data</td>
</tr>
<tr>
<td><code>count</code></td>
<td>packets.</td>
</tr>
<tr>
<td><code>rssi-threshold</code></td>
<td>Specifies 802.11 minimum-receive-coverage level for voice packets.</td>
</tr>
<tr>
<td><code>threshold</code></td>
<td></td>
</tr>
<tr>
<td><code>exceptional</code></td>
<td>Specifies 802.11 Cisco APs coverage-exception level. The range is between</td>
</tr>
<tr>
<td><code>global</code></td>
<td>0 and 100 percent.</td>
</tr>
<tr>
<td><code>value</code></td>
<td></td>
</tr>
<tr>
<td><code>level</code></td>
<td>Specifies 802.11 Cisco AP client-minimum-exception level between 1 and</td>
</tr>
<tr>
<td><code>global</code></td>
<td>75 clients.</td>
</tr>
<tr>
<td><code>value</code></td>
<td></td>
</tr>
<tr>
<td><code>voice</code></td>
<td>Specifies 802.11 coverage Hole-Detection for voice packets.</td>
</tr>
<tr>
<td><code>fail-percentage</code></td>
<td>Specifies 802.11 coverage failure rate threshold for uplink voice packets.</td>
</tr>
<tr>
<td><code>percentage</code></td>
<td></td>
</tr>
<tr>
<td><code>packet-count</code></td>
<td>Specifies 802.11 coverage minimum-uplink-failure count threshold for voice</td>
</tr>
<tr>
<td><code>packet-count</code></td>
<td>packets.</td>
</tr>
<tr>
<td><code>rssi-threshold</code></td>
<td>Specifies 802.11 minimum receive coverage level for voice packets.</td>
</tr>
<tr>
<td><code>threshold</code></td>
<td></td>
</tr>
</tbody>
</table>

**Command Default**

None.

**Command Modes**

Interface configuration.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>3.2SE</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

If both the number and percentage of failed packets exceed the values that you entered in the `ap dot11 {24ghz | 5ghz} rrm coverage packet-count` and `ap dot11 {24ghz | 5ghz} rrm coverage fail-percentage` commands for a 5-second period, the client is considered to be in a pre-alarm condition. The device uses this information to distinguish between real and false coverage holes and excludes clients with poor roaming logic. A coverage hole is detected if both the number and percentage of failed clients meet or exceed the values entered in the
The device determines whether the coverage hole can be corrected and, if appropriate, mitigate the coverage hole by increasing the transmit power level for that specific access point.

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

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

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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>24ghz</code></td>
<td>Specifies the 2.4 GHz band.</td>
</tr>
<tr>
<td><code>5ghz</code></td>
<td>Specifies the 5 GHz band.</td>
</tr>
<tr>
<td><code>controller-name</code></td>
<td>Name of the device to be added.</td>
</tr>
<tr>
<td><code>controller-ip</code></td>
<td>IP address of the device to be added.</td>
</tr>
</tbody>
</table>

**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 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

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

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

```
ap dot11 {5ghz|24ghz} rrm group-mode {auto|leader|off|restart}
oap dot11 {5ghz|24ghz} rrm group-mode
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5ghz</td>
<td>Specifies the 2.4 GHz band.</td>
</tr>
<tr>
<td>24ghz</td>
<td>Specifies the 5 GHz band.</td>
</tr>
<tr>
<td>auto</td>
<td>Sets the 802.11 RF group selection to automatic update mode.</td>
</tr>
<tr>
<td>leader</td>
<td>Sets the 802.11 RF group selection to static mode, and sets this device as the group leader.</td>
</tr>
<tr>
<td>off</td>
<td>Sets the 802.11 RF group selection to off.</td>
</tr>
<tr>
<td>restart</td>
<td>Restarts the 802.11 RF group selection.</td>
</tr>
</tbody>
</table>

### Command Default

auto

### Command Modes

Global configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

```
Device(config)# ap dot11 5ghz rrm group-mode auto
```
To configure report log settings on supported 802.11 networks, use the `ap dot11 rrm logging` command.

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

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

**Command Default**
- Disabled

**Command Modes**
- Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

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

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

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

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

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

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

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

This example shows how to turn the 5 GHz noise profile logging mode on:
Device(config)# ap dot11 5ghz rrm logging noise

This example shows how to turn the 5 GHz performance profile logging mode on:
Device(config)# ap dot11 5ghz rrm logging performance

This example shows how to turn the 5 GHz transmit power change mode on:
Device(config)# ap dot11 5ghz rrm logging txpower
**ap dot11 rrm monitor**

To configure monitor settings on the 802.11 networks, use the `ap dot11 rrm monitor` command.

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

**Syntax Description**

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

**Command Default**

None

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

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

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

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

To configure the 802.11 access point radio resource management neighbor discovery protocol type, use the **ap dot11 rrm ndp-type** command.

```
ap dot11 {24ghz|5ghz} rrm ndp-type {protected|transparent}
```

**Syntax Description**

- **24ghz**: Specifies the 2.4 GHz band.
- **5ghz**: Specifies the 5 GHz band.
- **protected**: Specifies the Tx RRM protected (encrypted) neighbor discovery protocol.
- **transparent**: Specifies the Tx RRM transparent (not encrypted) neighbor discovery protocol.

**Command Default**

None

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Before you configure the 802.11 access point RRM neighbor discovery protocol type, ensure that you have disabled the network by entering the **ap dot11 {24ghz | 5ghz} shutdown** command.

This example shows how to enable the 802.11a access point RRM neighbor discovery protocol type as protected:

```
Device(config)# ap dot11 5ghz rrm ndp-type protected
```
ap dot11 rrm tpc-threshold

To configure the tx-power control threshold used by RRM for auto power assignment, use the `ap dot11 rrm tpc-threshold` command. To disable, use the `no` form of the command.

```
ap dot11 \{24ghz|5ghz\} rrm tpc-threshold value
no ap dot11 \{24ghz|5ghz\} rrm tpc-threshold
```

**Syntax Description**

- `value` Specifies the power value. The range is between -80 and -50.

**Command Default**

None.

**Command Modes**

Interface configuration.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

None.

This example shows how to configure the tx-power control threshold used by RRM for auto power assignment.

```
Device#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)#ap dot11 5ghz rrm tpc-threshold -60
```
**ap dot11 rrm txpower**

To configure the 802.11 tx-power level, use the `ap dot11 rrm txpower` command. To disable the 802.11 tx-power level, use the `no` form of the command.

```plaintext
ap dot11 {24ghz|5ghz} rrm txpower {auto|max powerLevel|min powerLevel|once power-level}
noap dot11 {24ghz|5ghz} rrm txpower {auto|max powerLevel|min powerLevel|once power-level}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto</td>
<td>Enables auto-RF.</td>
</tr>
<tr>
<td>max powerLevel</td>
<td>Configures maximum auto-RF tx power. The range is between -10 to -30.</td>
</tr>
<tr>
<td>min powerLevel</td>
<td>Configures minimum auto-RF tx power. The range is between -10 to -30.</td>
</tr>
<tr>
<td>once</td>
<td>Enables one-time auto-RF.</td>
</tr>
</tbody>
</table>

**Command Default**

None.

**Command Modes**

Interface configuration.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE 3.3SE</td>
<td>The <code>no</code> form of the command is introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

None.

This example shows how to enables auto-RF once.

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

To configure the 802.11 tx-power level, use the `ap dot11 rrm txpower` command. To disable the 802.11 tx-power level, use the `no` form of the command.

```
ap dot11 {24ghz|5ghz} rrm txpower {auto|max powerLevel|min powerLevel|once power-level}
noap dot11 {24ghz|5ghz} rrm txpower {auto|max powerLevel|min powerLevel|once power-level}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>auto</th>
<th>Enables auto-RF.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>max powerLevel</td>
<td>Configures maximum auto-RF tx power. The range is between -10 to -30.</td>
</tr>
<tr>
<td></td>
<td>min powerLevel</td>
<td>Configures minimum auto-RF tx power. The range is between -10 to -30.</td>
</tr>
<tr>
<td></td>
<td>once</td>
<td>Enables one-time auto-RF.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>Interface configuration.</td>
</tr>
<tr>
<td>Command History</td>
<td></td>
</tr>
<tr>
<td>Release</td>
<td>Modification</td>
</tr>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE 3.3SE</td>
<td>The <code>no</code> form of the command is introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Usage Guidelines</th>
<th>None.</th>
</tr>
</thead>
</table>

This example shows how to enables auto-RF once.

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

To configure the AP filter and set the priority, use the `ap filter` command.

```
ap filter { { name filter-name } | { priority priority-number | filter-name filter-name } }
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>priority</td>
<td>Set the priority for a name filter.</td>
<td></td>
</tr>
<tr>
<td>priority-number</td>
<td>The valid AP filter priority range is 0 to 127.</td>
<td></td>
</tr>
<tr>
<td>filter-name</td>
<td>Enter the name for the ap filter.</td>
<td></td>
</tr>
</tbody>
</table>

Command Default

None

Command Modes

Global configuration (config)

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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

Examples

The following example shows how to create a ap filter and set the priority to this filter:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# ap filter namep-filter-name1
Device(config-aaa-policy)# aaa-realm enable
```
To configure flexible radio assignment (FRA) and its parameters, use the `ap fra` command.

```
ap fra[ :interval no-of-hours |sensitivity {high | low | medium} |sensor-threshold {balanced | client-preferred | client-priority | sensor-preferred | sensor-priority} |service-priority {coverage |service-assurance} ]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interval</code> no-of-hours</td>
<td>Enter the number of hours for the FRA interval. Valid range is 1 to 24 hours.</td>
</tr>
<tr>
<td><code>sensitivity</code> high</td>
<td>Configures the FRA coverage overlap sensitivity as high.</td>
</tr>
<tr>
<td></td>
<td>low</td>
</tr>
<tr>
<td></td>
<td>medium</td>
</tr>
<tr>
<td><code>sensor-threshold</code> balanced</td>
<td>Configures FRA sensor threshold to one of the available options.</td>
</tr>
<tr>
<td></td>
<td>client-preferred</td>
</tr>
<tr>
<td></td>
<td>client-priority</td>
</tr>
<tr>
<td></td>
<td>sensor-preferred</td>
</tr>
<tr>
<td></td>
<td>sensor-priority</td>
</tr>
<tr>
<td><code>service-priority</code> coverage</td>
<td>Configures FRA service priority to Coverage or Service Assurance.</td>
</tr>
<tr>
<td></td>
<td>service-assurance</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

`config`

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Ensure that the RF group leader for 802.11b/g and 802.11a bands are same across RF domain and make sure that the RF group leader has FRA enabled.

**Examples**

The following example show how to configure the FRA interval to 8 hours:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# ap fra interval 8
```
To configure hyperlocation and related parameters, use the **ap hyperlocation** command. To disable hyperlocation and related parameters, use the **no** form of this command.

```
ap hyperlocation  [ble-beacon {beacon-id | interval interval-value} | threshold {detection value-in-dBm | reset value-btwn-0-99 | trigger value-btwn-1-100}] [no] ap hyperlocation  [ble-beacon {beacon-id | interval interval-value} | threshold {detection value-in-dBm | reset value-btwn-0-99 | trigger value-btwn-1-100}]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ble-beacon</strong></td>
<td>Enables BLE beacon parameters.</td>
</tr>
<tr>
<td><strong>beacon-id</strong></td>
<td>BLE beacon ID. The range is from 1 to 4.</td>
</tr>
<tr>
<td><strong>interval</strong></td>
<td>Sets the BLE beacon interval.</td>
</tr>
<tr>
<td><strong>interval-value</strong></td>
<td>BLE beacon interval value, in hertz. The range is from 1 to 10. The default is 1.</td>
</tr>
<tr>
<td><strong>threshold detection</strong></td>
<td>Sets threshold to filter out packets with low RSSI. The [no] form of the command resets the threshold to its default value.</td>
</tr>
<tr>
<td><strong>threshold reset</strong></td>
<td>Resets value in scan cycles after trigger. The [no] form of the command resets the threshold to its default value.</td>
</tr>
<tr>
<td><strong>threshold trigger</strong></td>
<td>Sets the number of scan cycles before sending a BAR to clients. The [no] form of the command resets the threshold to its default value.</td>
</tr>
</tbody>
</table>

**Note** Ensure that the hyperlocation threshold reset value is less than the threshold trigger value.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Denali 16.2.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Denali 16.3.1</td>
<td>This command was modified. The <strong>ble-beacon</strong> keyword was added.</td>
</tr>
</tbody>
</table>
To configure an image on all access points that are associated to the device, use the `ap image` command.

```
ap image {predownload|reset|swap}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>predownload</code></td>
<td>Instructs all the access points to start predownloading an image.</td>
</tr>
<tr>
<td><code>reset</code></td>
<td>Instructs all the access points to reboot.</td>
</tr>
<tr>
<td><code>swap</code></td>
<td>Instructs all the access points to swap the image.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

Any command mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

This example shows how to predownload an image to all access points:

```
Device# ap image predownload
```

This example shows how to reboot all access points:

```
Device# ap image reset
```

This example shows how to swap the access point’s primary and secondary images:

```
Device# ap image swap
```
### ap image upgrade

To instruct all the APs to start image upgrade, use the `ap image upgrade` command.

```
ap image upgrade [{abort | destination controller-name {controller-ipv4-addr controller-ipv6-addr } | dry-run}]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>abort</td>
<td>Aborts AP image upgrade.</td>
</tr>
<tr>
<td>destination controller-name {controller-ipv4-addr</td>
<td>controller-ipv6-addr}</td>
</tr>
<tr>
<td>dry-run</td>
<td>Runs the rolling AP image upgrade in dry-run mode.</td>
</tr>
</tbody>
</table>

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to abort an AP image upgrade:

```
Device# ap image upgrade abort
```
ap link-encryption

To enable Datagram Transport Layer Security (DTLS) data encryption for access points, use the `ap link-encryption` command. To disable the DTLS data encryption for access points, use the `no ap link-encryption` form of this command.

```bash
ap link-encryption
no ap link-encryption
```

### Syntax Description
This command has no keywords and arguments.

### Command Default
Disabled

### Command Modes
Global configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

This example shows how to enable data encryption for all the access points that are joined to the controller:

```bash
Device(config)# ap link-encryption
```
ap name clear-personal-ssid

To clear the personal SSID from a Cisco OfficeExtend Access Point (OEAP), use the `ap name clear-personal-ssid` command.

```
ap name ap-name clear-personal-ssid
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ap-name</strong> AP name.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Modes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privileged EXEC</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Release</strong></td>
</tr>
<tr>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to clear the personal SSID from a Cisco OEAP:

```
Device# ap name my-oep clear-personal-ssid
```
ap name core-dump

To configure a Cisco lightweight access point’s memory core dump, use the `ap name core-dump` command. To disable a Cisco lightweight access point’s memory core dump, use the `no` form of this command.

```
ap name ap-name core-dump tftp-ip-addr filename {compress|uncompress}
nap name ap-name [no] core-dump
```

**Syntax Description**

- `ap-name`: Name of the access point.
- `tftp-ip-addr`: IP address of the TFTP server to which the access point sends core dump files.
- `filename`: Name that the access point used to label the core file.
- `compress`: Compresses the core dump file.
- `uncompress`: Uncompresses the core dump file.

**Command Default**

None

**Command Modes**

Any command mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The access point must be able to reach the TFTP server before you can use this command.

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

```
device# ap name AP2 core-dump 192.1.1.1 log compress
```
ap name crash-file

To manage crash data and radio core files for the Cisco access point, use the `ap name crash-file` command.

```
ap name ap-name crash-file {get-crash-data|get-radio-core-dump} {slot 0|slot 1}
```

**Syntax Description**

- **ap-name**
  - Name of the Cisco lightweight access point.

- **get-crash-data**
  - Collects the latest crash data for a Cisco lightweight access point.

- **get-radio-core-dump**
  - Gets a Cisco lightweight access point’s radio core dump

- **slot**
  - Slot ID for Cisco access point.
  - **0**
    - Specifies Slot 0.
  - **1**
    - Specifies Slot 1.

**Command Default**
None

**Command Modes**
Any command mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

```
Device# ap name AP3 crash-file get-crash-data
```

This example shows how to collect the radio core dump for access point AP02 and slot 0:

```
Device# ap name AP02 crash-file get-radio-core-dump slot 0
```
ap name dot11 dual-band cleanair

To configure CleanAir for a dual band radio, use the `ap name dot11 dual-band cleanair` command.

```
ap name ap-name dot11 dual-band cleanair
ap name ap-name no dot11 dual-band cleanair
```

**Syntax Description**

- **ap-name** Name of the Cisco AP.
- **cleanair** Specifies the CleanAir feature.

**Command Default**

None

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.3SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

This example shows how to enable CleanAir for a dual band radio of the access point AP01:

```
Device# ap name AP01 dot11 dual-band cleanair
```
ap name dot11 dual-band shutdown

To disable dual band radio on a Cisco AP, use the ap name dot11 dual-band shutdown command.

```
ap name ap-name dot11 dual-band shutdown
ap name ap-name no dot11 dual-band shutdown
```

**Syntax Description**

<table>
<thead>
<tr>
<th>ap-name</th>
<th>Name of the Cisco AP.</th>
</tr>
</thead>
<tbody>
<tr>
<td>shutdown</td>
<td>Disables the dual band radio on the Cisco AP.</td>
</tr>
</tbody>
</table>

**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 3.3SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

This example shows how to disable dual band radio on the Cisco access point AP01:

```
Device# ap name AP01 dot11 dual-band shutdown
```
ap name dot11 rrm profile

To configure Radio Resource Management (RRM) performance profile settings for a Cisco lightweight access point, use the **ap name dot11 rrm profile** command.

```
ap name ap-name dot11 {24ghz|5ghz} rrm profile {clients value|customize|foreign value|noise value|throughput value|utilization value}
```

### Syntax Description

- **ap-name**
  - Name of the Cisco lightweight access point.

- **24ghz**
  - Specifies the 2.4 GHz band.

- **5ghz**
  - Specifies the 5 GHz band.

- **clients**
  - Sets the access point client threshold.

- **value**
  - Access point client threshold from 1 to 75 clients.
  - **Note** The default client threshold is 12.

- **customize**
  - Turns on performance profile customization for an access point.
  - **Note** Performance profile customization is off by default.

- **foreign**
  - Sets the foreign 802.11 transmitter interference threshold.

- **value**
  - Foreign 802.11 transmitter interference threshold from 0 to 100 percent.
  - **Note** The default is 10 percent.

- **noise**
  - Sets the 802.11 foreign noise threshold.

- **value**
  - 802.11 foreign noise threshold between –127 and 0 dBm.
  - **Note** The default is –70 dBm.

- **throughput**
  - Sets the data-rate throughput threshold.

- **value**
  - 802.11 throughput threshold from 1000 to 10000000 bytes per second.
  - **Note** The default is 1,000,000 bytes per second.

- **utilization**
  - Sets the RF utilization threshold.

  **Note** The operating system generates a trap when this threshold is exceeded.

- **value**
  - 802.11 RF utilization threshold from 0 to 100 percent.
  - **Note** The default is 80 percent.
<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>Any command mode</td>
</tr>
<tr>
<td>Command History</td>
<td>Release</td>
</tr>
<tr>
<td></td>
<td>Cisco IOS XE 3.2SE</td>
</tr>
</tbody>
</table>

This example shows how to set the AP1 clients threshold to 75 clients:

```
Device# ap name AP1 dot11 24ghz rrm profile clients 75
```

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

```
Device# ap name AP1 dot11 5ghz rrm profile customize
```

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

```
Device# ap name AP1 dot11 5ghz rrm profile foreign 0
```

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

```
Device# ap name AP1 dot11 5ghz rrm profile noise 0
```

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

```
Device# ap name AP1 dot11 5ghz rrm profile throughput 10000000
```

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

```
Device# ap name AP1 dot11 5ghz rrm profile utilization 100
```
To configure hyperlocation and related parameters for an access point (AP), use the `ap name hyperlocation` command. To disable hyperlocation and related parameters, use the `no` form of this command.

```
ap name \ap-name\ hyperlocation ble-beacon \beacon-id\ \{ major \major-value\ | minor \minor-value\ | txpwr \att-value\ }
```

### Syntax Description
- **ap-name** Access point name.
- **ble-beacon** Configures BLE beacon parameters.
- **beacon-id** BLE beacon ID.
- **major** Configures BLE beacon major parameter.
- **major-value** BLE beacon major value. The range is from 0 to 65535. The default is 0.
- **minor** Configures BLE beacon minor parameter.
- **minor-value** BLE beacon minor value. The range is from 0 to 65535. The default is 0.
- **txpwr** Configures BLE beacon attenuation level.
- **att-value** BLE beacon attenuation value, in dBm. The range is from 0 to 52. The default is 0.

### Command Default
BLE beacon details are not configured.

### Command Modes
Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Denali 16.3.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Example
This example shows how to configure hyperlocation and related parameters for an AP:

```
Controller# ap name test-ap hyperlocation ble-beacon 3 txpwr 50
```
**ap name mesh block-child**

To set mesh block-child state for a mesh AP, use the **ap name mesh block-child** command.

```
ap name ap-name mesh block-child
```

**Syntax Description**

- `ap-name` Name of the mesh AP.

**Command Default**

None

**Command Modes**

Privileged EXEC

**Command History**

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

**Examples**

The following example shows how to configure the mesh block-child state for a mesh AP:

```
Device # ap name mymeshap mesh block-child
```
ap name mesh daisy-chaining

To configure daisy-chain mode for a mesh AP, use the **ap name ap-name mesh daisy-chaining** command.

```
ap name ap-name mesh daisy-chaining [{strict-rap}]
```

**Syntax Description**

- **ap-name** Name of the mesh AP.
- **strict-rap** Configures to allow only the Ethernet interface as mesh uplink.

**Command Default**

None

**Command Modes**

Privileged EXEC

**Command History**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure daisy-chaining mode for a mesh AP:

```
Device # ap name mymeshap mesh daisy-chaining
```
ap name mesh ethernet mode access

To configure the mode of Ethernet interface as access for a mesh AP, use the `ap name ap-name mesh ethernet port-no mode access` command.

```
ap name ap-name mesh ethernet port-no mode access vlan-id
```

**Syntax Description**

- `ap-name`: Name of the mesh AP.
- `port-no`: Port number of the AP. Valid options are 1, 2, 3, and 4.
- `vlan-id`: VLAN ID. Valid range is from 0 to 4095.

**Command Default**

None

**Command Modes**

Privileged EXEC

**Command History**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure the mode of Ethernet interface as access for a mesh AP:

```
Device # ap name mymeshap mesh ethernet 0 mode access 10
```
ap name mesh ethernet mode trunk

To configure the mode of Ethernet interface as trunk for a mesh AP, use the `ap name ap-name mesh ethernet port-no mode trunk` command.

```
ap name ap-name mesh ethernet port-no mode trunk vlan {allowed |native} vlan-id
```

**Syntax Description**

- `ap-name` Name of the mesh AP.
- `port-no` Port number of the AP. Valid options are 1, 2, 3, and 4.
- `allowed` Configures allowed VLANs for the trunk port.
- `native` Configures native VLAN for the trunk port.
- `vlan-id` VLAN ID. Valid range for allowed VLANs is from 0 to 4095. Valid range for native VLANs is 1 to 4095.

**Command Default**

None

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
</table>
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

**Examples**

The following example shows how to configure the mode of Ethernet interface as trunk for a mesh AP and also configure allowed VLANs for the trunk port:

```
Device # ap name mymeshap mesh ethernet 0 mode trunk vlan allowed 10
```
**ap name mesh linktest**

To perform a link test with a mesh AP, use the **ap name ap-name mesh linktest** command.

```
ap name ap-name mesh linktest dest-ap-mac data-rate pkts-per-sec pkt-size test-duration
```

### Syntax Description

- **ap-name**: Name of the mesh AP.
- **dest-ap-mac**: MAC address of the destination mesh AP.
- **data-rate**: Data rate in Mbps (1, 2, 5.5, 6, 9, 11, 12, 24, 36, 48, 53, m0-m15)
- **pkts-per-sec**: Packets to be sent per second. Valid range is from 1 to 25000.
- **pkt-size**: Packet size. Valid range is from 1 to 1500.
- **test-duration**: Test duration. Valid range is from 10 to 300 seconds.

### Command Default

None

### Command Modes

Privileged EXEC

### Command History

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

### Examples

The following example shows how to configure a link test for a mesh AP:

```
Device # ap name mymeshap mesh linktest 00c0.00a0.3fa.0000.0000
       9 100 10 180
```
**ap name mesh parent preferred**

To configure preferred parent for a mesh AP, use the `ap name ap-name mesh parent preferred` command.

```
ap name ap-name mesh parent preferred mac-address
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ap-name</strong></td>
<td>Name of the mesh AP.</td>
</tr>
<tr>
<td><strong>mac-address</strong></td>
<td>Radio MAC address of the parent AP.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>Privileged EXEC</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<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>

**Examples**

The following example shows how to preferred parent for a mesh AP:

```
Device # ap name mymeshap mesh parent preferred dc:5f:be:f5:fd:84
```
**ap name mesh security psk provision delete**

To delete PSK-provisioned key from a mesh AP, use the `ap name ap-name mesh security psk provision delete` command.

```
ap name ap-name mesh security psk provision delete
```

**Syntax Description**
- `ap-name`: Name of the mesh 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 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>

**Examples**

The following example shows how to delete PSK-provisioned key from a mesh AP:

```
Device # ap name mymeshap mesh security psk provision delete
```
**ap name mesh vlan-trunking native**

To configure vlan trunking for bridge mode AP, use the `ap name ap-name mesh vlan-trunking native` command.

```
ap name rap-name mesh vlan-trunking native vlan-id
```

**Syntax Description**

- **ap-name**: Name of the Root AP (RAP).
- **native**: Native VLAN for Mesh AP.
- **vlan-id**: VLAN ID. Valid range is from 01 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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure VLAN trunking on a mesh AP:

```
Device # ap name mymeshap mesh vlan-trunking native 10
```
# ap name mesh vlan-trunking native

To configure native VLAN for mesh AP, use the `ap name mesh vlan-trunking native` command.

```plaintext
ap name name-of-rap vlan-trunking native vlan-id
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>name-of-rap</strong></td>
</tr>
<tr>
<td><strong>vlan-id</strong></td>
</tr>
</tbody>
</table>

| 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>

### Example

The following example shows how to configure native VLAN for mesh AP:

```
Device # ap name mesh vlan-trunking native 12
```
To change a Cisco device communication option for an individual Cisco lightweight access point, use the `ap name mode` command.

```plaintext
ap name ap-name mode {local submode {none|wips}|monitor submode {none|wips}|rogue|se-connect|sniffer}
```

**Syntax Description**
- **ap-name**: Name of the Cisco lightweight access point.
- **local**: Converts from an indoor mesh access point (MAP or RAP) to a nonmesh lightweight access point (local mode).
- **submode**: Specifies wIPS submode on an access point.
- **none**: Disables the wIPS on an access point.
- **monitor**: Specifies monitor mode settings.
- **wips**: Enables the wIPS submode on an access point.
- **rogue**: Enables wired rogue detector mode on an access point.
- **se-connect**: Enables spectrum expert mode on an access point.
- **sniffer**: Enables wireless sniffer mode on an access point.

**Command Default**
Local

**Command Modes**
Any command mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
The sniffer mode captures and forwards all the packets from the clients on that channel to a remote machine that runs AiroPeek or other supported packet analyzer software. It includes information on the timestamp, signal strength, packet size and so on.

This example shows how to set the device to communicate with access point AP01 in local mode:
```plaintext
Device# ap name AP01 mode local submode none
```

This example shows how to set the device to communicate with access point AP01 in a wired rogue access point detector mode:
```plaintext
Device# ap name AP01 mode rogue
```

This example shows how to set the device to communicate with access point AP02 in wireless sniffer mode:
Device# ap name AP02 mode sniffer
**ap name mode bridge**

To configure Bridge mode for an AP, use the `ap name ap-name mode bridge` command.

```
ap name ap-name mode bridge
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ap-name</code></td>
<td>Name of the AP.</td>
</tr>
</tbody>
</table>

| Command Default   | None |

| Command Modes     | Privileged EXEC |

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<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>

**Examples**

The following example shows how to configure a Bridge mode for an AP:

```
Device # ap name my-ap mode bridge
```
**ap name monitor-mode**

To configure Cisco lightweight access point channel optimization, use the `ap name monitor-mode` command.

```
ap name ap-name monitor-mode {no-optimization|tracking-opt|wips-optimized}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ap-name</td>
<td>Name of the Cisco lightweight access point.</td>
</tr>
<tr>
<td>no-optimization</td>
<td>Specifies no channel scanning optimization for the access point.</td>
</tr>
<tr>
<td>tracking-opt</td>
<td>Enables tracking optimized channel scanning for the access point.</td>
</tr>
<tr>
<td>wips-optimized</td>
<td>Enables wIPS optimized channel scanning for the access point.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

Any command mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

This example shows how to configure a Cisco wireless intrusion prevention system (wIPS) monitor mode on access point AP01:

```
Device# ap name AP01 monitor-mode wips
```
ap name monitor-mode dot11b

To configure 802.11b scanning channels for a monitor-mode access point, use the **ap name monitor-mode dot11b** command.

```
ap name ap-name monitor-mode dot11b fast-channel channel1 [channel2] [channel3] [channel4]
```

**Syntax Description**

- **ap-name** Name of the access point.
- **fast-channel** Specifies the 2.4 GHz band scanning channel (or channels) for a monitor-mode access point.
  - **channel1** Scanning channel1.
  - **channel2** (Optional) Scanning channel2.
  - **channel3** (Optional) Scanning channel3.
  - **channel4** (Optional) Scanning channel4.

**Command Default**

None

**Command Modes**

Any command mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

This example shows how to configure an access point in tracking optimized mode to listen to channels 1, 6, and 11:

```
Device# ap name AP01 monitor-mode dot11b fast-channel 1 6 11
```
**ap name priority**

To configure the priority of an access point, use the `ap name priority` command.

```
ap name ap-name priority priority-value
```

**Syntax Description**

- `priority-value` Priority value for the AP. Valid range is 1 to 4.

**Command Default**

None

**Command Modes**

Privileged EXEC

**Command History**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure the priority for an access point:

```
Device# ap name my-ap priority 1
```
ap name role

To configure the role of operation for an AP, use the **ap name role** command.

```
ap name ap-name role {mesh-ap | root-ap}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ap-name</strong></td>
<td>Name of the AP</td>
</tr>
<tr>
<td><strong>mesh-ap</strong></td>
<td>Configures mesh AP role for the AP.</td>
</tr>
<tr>
<td><strong>root-ap</strong></td>
<td>Configures root AP role for the AP.</td>
</tr>
</tbody>
</table>

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure the role of operation as mesh AP for an AP:

```
Device # ap name mymeshap role mesh-ap
```
**ap name shutdown**

To disable a Cisco lightweight access point, use the `ap name shutdown` command. To enable a Cisco lightweight access point, use the `no` form of this command.

```
ap name ap-name shutdown
ap name ap-name no shutdown
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>ap-name</th>
<th>Name of the Cisco lightweight access point.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Default</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Command Modes</td>
<td>Any command mode</td>
<td></td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

This example how to disable a specific Cisco lightweight access point:

```
Device# ap name AP2 shutdown
```
ap name sniff

To enable sniffing on an access point, use the **ap name sniff** command. To disable sniffing on an access point, use the **no** form of this command.

```
ap name ap-name sniff {dot11a|dot11b}
ap name ap-name no sniff {dot11a|dot11b}
```

**Syntax Description**

- **ap-name**  
  Name of the Cisco lightweight access point.

- **dot11a**  
  Specifies the 2.4 GHz band.

- **dot11b**  
  Specifies the 5 GHz band.

- **channel**  
  Valid channel to be sniffed. For the 5 GHz band, the range is 36 to 165. For the 2.4 GHz band, the range is 1 to 14.

- **server-ip-address**  
  IP address of the remote machine running Omnitek, Airopeek, AirMagnet, or Wireshark software.

**Command Default**

Channel 36

**Command Modes**

Any command mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE</td>
<td></td>
</tr>
<tr>
<td>3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When the sniffer feature is enabled on an access point, it starts sniffing the signal on the given channel. It captures and forwards all the packets to the remote computer that runs Omnitek, Airopeek, AirMagnet, or Wireshark software. It includes information about the timestamp, signal strength, packet size and so on.

Before an access point can act as a sniffer, a remote computer that runs one of the listed packet analyzers must be set up so that it can receive packets that are sent by the access point.

This example shows how to enable the sniffing on the 5 GHz band for an access point on the primary wireless LAN controller:

```
Device# ap name AP2 sniff dot11a 36 192.0.2.54
```
### ap name tftp-downgrade

To configure the settings used for downgrading a lightweight access point to an autonomous access point, use the **ap name tftp-downgrade** command.

```
ap name ap-name tftp-downgrade tftp-server-ip filename
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ap-name</td>
<td>Name of the Cisco lightweight access point.</td>
</tr>
<tr>
<td>tftp-server-ip</td>
<td>IP address of the TFTP server.</td>
</tr>
<tr>
<td>filename</td>
<td>Filename of the access point image file on the TFTP server.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>Any command mode</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

This example shows how to configure the settings for downgrading access point AP1:

```
Device# ap name Ap01 tftp-downgrade 172.21.12.45 ap3g1-k9w7-tar.124-25d.JA.tar
```
To configure VLAN tagging for a nonbridge AP, use the `ap name vlan-tag` command.

```
ap name ap-name vlan-tag vlan-id
```

**Syntax Description**
- `ap-name` Access point name.
- `vlan-id` VLAN identifier.

**Command Default**
VLAN tagging is not enabled.

**Command Modes**
Privileged EXEC

**Command History**

<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>

**Example**

The following example shows how to configure VLAN tagging for a nonbridge AP:

```
Device# ap name AP1 vlan-tag 12
```
**ap name write tag-config**

To write the existing configuration to an AP, use the `ap name write tag-config` command in privileged EXEC mode

```
ap name  ap-name write tag-config
```

**Syntax Description**

- **ap-name**: Name of the access point.

**Command Default**

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>

**Usage Guidelines**

Use this command to write the existing configuration to an AP.

**Example**

This example shows how to write the existing configuration to an AP:

```
Device# ap name AP40CE.2485.D594 write tag-config
```
**ap name-regex**

To configure filter based on AP name regular expression to match with, use the `ap name-regex` command.

```
ap name-regex regular-expression
```

**Syntax Description**

| regular-expression | Enter the filter string. |

**Command Default**

None

**Command Modes**

config-ap-filter

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure filter based on AP name regular expression match with:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# ap filter name filter--name
Device(config-ap-filter)# ap name-regex regular-expression-string
```
ap packet-capture

To start or stop the AP packet capture process, use the **ap packet-capture** command.

```
ap packet-capture {start | stop} client-mac-address {auto | static ap-name}
```

**Syntax Description**

- `client-mac-address`: Client MAC address.
- `ap-name`: AP name.

**Command Default**

None

**Command Modes**

Privileged EXEC

**Command History**

<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>

**Usage Guidelines**

When using the `stop` option with **ap packet capture** command, use the keyword **all** to stop the packet capture.

**Example**

The following example shows how to start the AP packet capture process:

```
Device# ap packet-capture start 3c08.f672.1ad9 static AP_2029
```

The following example shows how to stop the AP packet capture process fully:

```
Device# ap packet-capture stop 3c08.f672.1ad9 all
```
ap packet-capture profile

To configure the AP packet capture profile, use the `ap packet-capture profile` command.

`ap packet-capture profile  profile-name`

**Syntax Description**

- `profile-name`  AP packet capture profile name.

**Command Default**

None

**Command Modes**

Privileged EXEC

**Command History**

<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>

**Example**

The following example shows how to configure the AP packet capture profile:

```
Device# ap packet-capture profile test1
```
ap packet-capture start

To enable packet capture for the specified client on a set of nearby access points, use the `ap packet-capture start` command.

```
ap packet-capture start client-mac-addr {auto | static ap-name}
```

**Syntax Description**

- `client-mac-addr`  MAC address of the client whose packet capture has to be done.
- `auto`  Starts packet capture in the nearby APs.
- `static ap-name`  Name of the AP in which the packet capture has to be done.

**Command Default**

None

**Command Modes**

Privileged EXEC

**Command History**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enable packet capture for a client on a set of nearby access points:

```
Device# ap packet-capture start 0011.0011.0011 auto
```
To configure access point profile, use the **ap profile** command.

```
ap profile  profile-name
```

**Syntax Description**

| profile-name | Enter the name of the AP profile. |

**Command Default**

By default, the AP profile name is default-ap-profile.

**Command Modes**

Global configuration (config)

**Command History**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure AP profile name:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# ap profile my-ap-profile
```
ap remote-lan profile-name

To configure remote LAN profile, use the `ap remote-lan profile-name` command.

```
ap remote-lan profile-name remote-lan-profile-name rlan-id
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>remote-lan-profile-name</code></td>
<td>Is the remote LAN profile name. Range is from 1 to 32 alphanumeric characters.</td>
</tr>
<tr>
<td><code>rlan-id</code></td>
<td>Is the remote LAN identifier. Range is from 1 to 128.</td>
</tr>
</tbody>
</table>

**Note**

You can create a maximum of 128 RLANs. You cannot use the `rlan-id` of an existing RLAN while creating another RLAN.

Both RLAN and WLAN profile cannot have the same names. Similarly, RLAN and WLAN policy profile cannot have the same names.

**Command Default**

None

**Command Modes**

Global configuration (config)

**Command History**

<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>

This example shows how to configure remote LAN profile:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# ap remote-lan profile-name rlan_profile_name 3
```
ap remote-lan shutdown

To enable or disable all RLANs, use the `ap remote-lan shutdown` command.

Command Default
None

Command Modes
Global configuration (config)

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>

Example

This example shows how to enable or disable all RLANs:

```plaintext
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# [no] ap remote-lan shutdown
Device(config)# end
```
ap remote-lan-policy policy-name

To configure RLAN policy profile, use the `ap remote-lan-policy policy-name` command.

```
ap remote-lan-policy policy-name profile-name
```

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>Global configuration (config)</td>
</tr>
<tr>
<td>Command History</td>
<td>Release</td>
</tr>
<tr>
<td></td>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
</tr>
</tbody>
</table>

**Example**

This example shows how to configure RLAN policy profile:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# ap remote-lan-policy policy-name rlan_policy_prof_name
```
ap tag-source-priority

To configure ap tag source priority, use the **ap tag-source-priority** command.

**ap tag-source-priority source-priority source { filter | ap }**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>source-priority</td>
<td>Enter the ap tag source priority. Valid range is 2 to 3.</td>
</tr>
<tr>
<td>source</td>
<td>Specify the source for which priority is been set.</td>
</tr>
<tr>
<td>filter</td>
<td>AP filter as tag source.</td>
</tr>
<tr>
<td>ap</td>
<td>AP as tag source.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

config

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to set AP as a tag source:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# ap tag-source-priority priority-value source ap
Device
```
ap tag-sources revalidate

To revalidate the access point tag sources, use the `ap tag-sources revalidate` command.

```
ap tag-sources revalidate
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>tag-sources</code></td>
</tr>
<tr>
<td><code>revalidate</code></td>
</tr>
</tbody>
</table>

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to revalidate the access point tag sources:

```
Device# ap tag-sources revalidate
```
**ap vlan-tag**

To configure VLAN tagging for all non-bridge APs, use the `ap vlan-tag` command.

**ap vlan-tag  vlan-id**

**Syntax Description**

| **vlan-id** | VLAN identifier. |

**Command Default**

VLAN tagging is not enabled for non-bridge APs.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th><strong>Release</strong></th>
<th><strong>Modification</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Example**

The following example shows how to configure VLAN tagging for all non-bridge APs:

```
Device# ap vlan-tag 1000
```
## arp-caching

To enable arp-caching, use the `arp-caching` command.

### Syntax Description

This command has no keywords or arguments.

### Command Default

None

### Command Modes

`config-wireless-flex-profile`

### 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>

### Example

The following example shows how to enable arp-caching:

```
Device(config-wireless-flex-profile)# arp-caching
```
assisted-roaming

To configure assisted roaming using 802.11k on a WLAN, use the `assisted-roaming` command. To disable assisted roaming, use the `no` form of this command.

```
assisted-roaming {dual-list|neighbor-list|prediction}
no assisted-roaming {dual-list|neighbor-list|prediction}
```

**Syntax Description**

- `dual-list` Configures a dual band 802.11k neighbor list for a WLAN. The default is the band that the client is currently associated with.
- `neighbor-list` Configures an 802.11k neighbor list for a WLAN.
- `prediction` Configures assisted roaming optimization prediction for a WLAN.

**Command Default**

Neighbor list and dual band support are enabled by default. The default is the band that the client is currently associated with.

**Command Modes**

WLAN configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.3SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When you enable the assisted roaming prediction list, a warning appears and load balancing is disabled for the WLAN if load balancing is already enabled on the WLAN. To make changes to the WLAN, the WLAN must be in disabled state.

**Example**

The following example shows how to configure a 802.11k neighbor list on a WLAN:

```
Device(config-wlan)#assisted-roaming neighbor-list
```

The following example shows the warning message when load balancing is enabled on a WLAN. Load balancing must be disabled if it is already enabled when configuring assisted roaming:

```
Device(config)#wlan test-prediction 2 test-prediction
Device(config-wlan)#client vlan 43
Device(config-wlan)#no security wpa
Device(config-wlan)#load-balance
Device(config-wlan)#assisted-roaming prediction
WARNING: Enabling neighbor list prediction optimization may slow association and impact VOICE client perform.
Are you sure you want to continue? (y/n)? y
% Request aborted - Must first disable Load Balancing before enabling Assisted Roaming Prediction Optimization on this WLAN.
```
auto qos

To enable Auto QoS Wireless Policy, use the `auto qos` command. To remove Auto QoS Wireless Policy, use the `no` form of this command.

```
auto qos enterprise | guest | voice
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>enterprise</code></td>
<td>Enables AutoQos Wireless Enterprise Policy.</td>
</tr>
<tr>
<td><code>guest</code></td>
<td>Enables AutoQos Wireless Guest Policy</td>
</tr>
<tr>
<td><code>voice</code></td>
<td>Enables AutoQos Wireless Voice Policy</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Command Modes</th>
<th>WLAN Configuration</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>This example shows how to enable AutoQos Wireless Enterprise Policy.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enter configuration commands, one per line. End with CNTL/Z.</td>
</tr>
<tr>
<td></td>
<td>Device(config)# wlan wlan1</td>
</tr>
<tr>
<td></td>
<td>Device(config-wlan)# auto qos enterprise</td>
</tr>
</tbody>
</table>
avg-packet-size packetsize

To configure the wireless media-stream's average packet size, use the **avg-packet-size** command.

```
avg-packet-size packetsize-value
```

**Syntax Description**

- **packetsize-value**: Average Packet Size. Valid range is 100 to 1500.

**Command Default**

None

**Command Modes**

media-stream

**Command History**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure wireless media-stream's average packet size:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless media-stream group doc-grp 224.0.0.0 224.0.0.223
Device(config-media-stream)# avg-packet-size 500
```
Avoid label exhaustion error

To avoid label exhaustion error happening on BGP routes during the time period when MSMR and fabric border are on two different nodes and any of those nodes is a catalyst 9300, use the `mpls label mode all-vrfs protocol all-afs per-vrf` command in global configuration mode.
backhaul (mesh)

To configure mesh backhaul for a mesh AP profile, use the backhaul command.

```
backhaul rate dot11 {24ghz | 5ghz} {auto | dot11abg rate | dot11n mcs mcs-index }
```

**Syntax Description**

- `rate` Backhaul transmission rate.
- `dot11` Specifies 802.11.
- `24ghz` Specifies 802.11b.
- `5ghz` Specifies 802.11a.
- `auto` Specifies method as auto.
- `dot11abg` Specifies method as dot11abg.
- `dot11n` Specifies method as dot11n.
- `mcs` Media convergence servers.
- `rate` Media convergence server rate.
- `mcs-index` Media convergence servers rate value for 802.11.

**Command Default**

Backhaul client access is disabled.

**Command Modes**

- `config-wireless-mesh-profile`

**Command History**

<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>

**Example**

The following example shows how to configure mesh backhaul details for a mesh AP profile:

```
Device # configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device (config)# wireless profile mesh mesh-profile
Device (config-wireless-profile)# backhaul rate dot11 24ghz auto
```
background-scanning (mesh)

To configure background scanning for a mesh AP profile, use the **background-scanning** command.

```
background-scanning
```

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

Background scanning is disabled.

**Command Modes**

config-wireless-mesh-profile

**Command History**

<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>

**Example**

The following example shows how to configure background scanning for a mesh AP profile:

Device # configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device (config)# wireless profile mesh mesh-profile
Device (config-wireless-mesh-profile)# background-scanning
band-select client

To configure the client threshold minimum dB for the selected band, use the `band-select client` command. To reset the client threshold minimum dB for the selected band, use the `no` form of this command.

```
band-select client {mid-rssi | rssi} dBm value
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mid-rssi</td>
<td>Minimum dBm of a client RSSI start to respond to probe</td>
</tr>
<tr>
<td>rssi</td>
<td>Minimum dBm of a client RSSI to respond to probe</td>
</tr>
<tr>
<td>dBm value</td>
<td>Minimum dBm of a client RSSI to respond to probe. Valid range is between -90 and -20 dBm.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

config-rf-profile

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Denali 16.3.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command is enabled only for 2.4-GHz band.

This example shows how to set the client threshold to minimum dB for a selected band.

```
Device(config-rf-profile)#band-select client rssi -50
```
band-select cycle

To configure the band cycle parameters, use the `band-select cycle` command. To reset the threshold value, use the `no` form of this command.

`band-select cycle { count | threshold } value`

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>count</td>
<td>Sets the Band Select probe cycle count.</td>
<td></td>
</tr>
<tr>
<td>value</td>
<td>Maximum number of cycles not responding. The range is between 1 and 10.</td>
<td></td>
</tr>
<tr>
<td>threshold</td>
<td>Sets the time threshold for a new scanning cycle.</td>
<td></td>
</tr>
<tr>
<td>value</td>
<td>Set the threshold value in milliseconds. The valid is between 1 and 1000.</td>
<td></td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

config-rf-profile

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Denali 16.3.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

None

This example shows how to configure the probe cycle count in an RF profile for a selected band.

```
Device(config-rf-profile)#band-select cycle count 5
```
band-select expire

To configure the expiry time for the RF profile for the selected band, use the `band-select expire` command. To reset the value, use the `no` form of this command.

```
band-select expire { dual-band | suppression } value
no band-select expire { dual-band | suppression }
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dual-band</td>
<td>Configures the RF Profile Band Select Expire Dual Band.</td>
</tr>
<tr>
<td>value</td>
<td>Setting the time to expire for pruning previously known dual-band clients. The range is between 10 and 300.</td>
</tr>
<tr>
<td>suppression</td>
<td>Configures the RF Profile Band Select Expire Suppression.</td>
</tr>
<tr>
<td>value</td>
<td>Setting the time to expire for pruning previously known 802.11b/g clients. The range is between 10 and 200.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

config-rf-profile

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Denali 16.3.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

None

This example shows how to configure the time to expire for a dual-band of an RF profile in a selected band.

```
Device(config-rf-profile)#band-select expire dual-band 15
```
band-select probe-response

To configure the probe responses to the clients for a selected band, use the `band-select probe-response` command. To disable the probe-response, use the `no` form of this command.

**Syntax Description**

- **probe-response**
  - Probe responses to clients.

**Command Default**

None

**Command Modes**

config-rf-profile

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Denali 16.3.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

None

This example shows how to enable probe response to the clients.

```
Device(config-rf-profile)# band-select probe-response
```
## bridge-group

To configure bridge group parameters for a mesh AP profile, use the `bridge-group` command.

```
bridge-group {name bridge-group-name | strict-match }
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Configures bridge group name.</td>
</tr>
<tr>
<td>bridge-group-name</td>
<td>Configures bridge group strict matching.</td>
</tr>
</tbody>
</table>

### Command Default

None

### Command Modes

config-wireless-mesh-profile

### 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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to configure the bridge group name for a mesh AP profile:

```
Device # configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device (config)# wireless profile mesh mesh-profile
Device (config-wireless-mesh-profile)# bridge-group name mesh-bridge-group
```
To configure BSS transition per WLAN, use the `bss-transition` command.

```plaintext
bss-transition  [ disassociation-imminent ]
```

**Syntax Description**
- `bss-transition`: BSS transition command.
- `disassociation-imminent`: BSS transition disassociation Imminent per WLAN.

**Command Default**
None

**Command Modes**
- config-wlan

**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>

**Example**

The following example shows how to configure BSS transition per WLAN:

```
Device(config-wlan)# bss-transition
```
battery-state (mesh)

To configure battery state for an AP, use the `battery-state` command.

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

**Command Default**
Battery state is enabled.

**Command Modes**
config-wireless-mesh-profile

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

**Example**

The following example shows how to configure battery state for an AP:

```
Device # configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device (config)# wireless profile mesh mesh-profile
Device (config-wireless-mesh-profile)# battery-state
```
cache timeout active value

To set the active flow monitor timeout value in seconds, use the cache timeout active value command.

```
cache timeout active value
```

**Syntax Description**

- `value` Enter the active timeout value. Valid range is 1 to 604800.

**Command Default**

None

**Command Modes**

- config-flow-monitor

**Command History**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to set the flow monitor inactive timeout value:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# flow monitor flow-monitor-name
Device(config-flow-monitor)# cache timeout active 300
```
cache timeout inactive value

To set the flow monitor inactive timeout value in seconds, use the `cache timeout inactive value` command.

**cache timeout inactive value**

**Syntax Description**

`value` Enter the inactive timeout value. Valid range is 1 to 604800.

**Command Default**

None

**Command Modes**

config-flow-monitor

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
</table>
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

**Examples**

The following example shows how to set the flow monitor inactive timeout value:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# flow monitor flow-monitor-name
Device(config-flow-monitor)# cache timeout inactive 300
```
call-snoop

call-snoop

no call-snoop

Syntax Description
This command has no keywords or arguments.

Command Default
VoIP snooping is disabled by default.

Command Modes
WLAN configuration

Command History

<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>

Usage Guidelines
You must disable the WLAN before using this command. The WLAN on which call snooping is configured must be configured with Platinum QoS. You must disable quality of service before using this command.

Example
This example shows how to enable VoIP on a WLAN:

```
Device# configure terminal
Device(config)# wireless profile policy policy-name
Device(config-wireless-policy)# service-policy input platinum-up
Device(config-wireless-policy)# service-policy output platinum
Device(config-wireless-policy)# call-snoop
Device(config-wireless-policy)# no shutdown
Device(config-wireless-policy)# end
```
captive-portal-bypass

To configure captive bypassing, use the captive-portal-bypass command.

**captive-portal-bypass**

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>Global configuration (config)</td>
</tr>
</tbody>
</table>

**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>

**Example**

This example shows how to configure captive bypassing for WLAN in LWA and CWA:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# parameter-map type webauth WLAN1_MAP
Device(config)# captive-portal-bypass
Device(config)# wlan WLAN1_NAME 4 WLAN1_NAME
Device(config-wlan)# security web-auth
Device(config-wlan)# security web-auth parameter-map WLAN1_MAP
Device(config-wlan)# end
```
To configure channel change notification for a mesh AP profile, use the `ccn` command.

```plaintext
ccn
```

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

**Command Default**
Channel change notification is disabled.

**Command Modes**
config-wireless-mesh-profile

**Command History**

<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>

**Example**

The following example shows how to configure channel change notification for a mesh AP profile:

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

To enable central association for locally switched clients, use the **central association** command.

```
central association
```

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

None

**Command Modes**

config-wireless-policy

**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>

**Example**

The following example shows how to enable enable central association for locally switched clients:

```
Device(config-wireless-policy)# central association
```
central authentication

To enable or disable central authentication, use the `central authentication` command.

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

None

**Command Modes**

config-wireless-policy

**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>

**Example**

The following example shows how to enable central authentication:

```
Device(config-wireless-policy)# central authentication
```
**central dhcp**

To enable central dhcp for locally switched clients, use the `central dhcp` command.

```plaintext
central dhcp
```

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

None

**Command Modes**

config-wireless-policy

**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>

**Example**

The following example shows how to enable central dhcp for locally switched clients:

```
Device(config-wireless-policy)# central dhcp
```
## central switching

To enable or disable central switching, use the `central switching` command.

### Syntax Description

This command has no keywords or arguments.

### Command Default

None

### Command Modes

`config-wireless-policy`

### 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>

### Example

The following example shows how to enable or disable central switching:

```plaintext
Device(config-wireless-policy)# central switching
```
To configure central-webauth for an ACL, use the `central-webauth` command.

**central-webauth**

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

**Command Default**
None

**Command Modes**
config-wireless-policy

**Command History**

<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>

**Example**
The following example shows how to configure central-webauth for an ACL:

```
Device(config-wireless-policy)# central-webauth
```
chassis clear

To clear persistent chassis information, use the **chassis clear** command.

```
chassis clear
```

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>Privileged EXEC</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release</td>
</tr>
<tr>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to clear persistent chassis information:

```
Device# chassis clear
```
chassis ha-interface

To configure the high availability (HA) interface for a chassis, use the chassis ha-interface command.

```
chassis ha-interface GigabitEthernet interface-number local-ip ip-address netmask remote-ip remote-chassis-ip-addr
```

**Syntax Description**

- **interface-number**
  - GigabitEthernet interface number. Valid range is 1 to 32.
- **local-ip ip-address netmask**
  - Configures the IP address of the local chassis HA interface. For the netmask, enter the netmask or the prefix length in the following formats: /nn or A.B.C.D.
- **remote-ip remote-chassis-ip-addr**
  - Configures the remote chassis IP address.

**Command Default**

None

**Command Modes**

Privileged EXEC

**Command History**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure the HA interface for a chassis:

```
Device# chassis ha-interface GigabitEthernet 2 local-ip 1.1.1.2 255.255.255.0 remote-ip 1.1.1.3
```
**chassis priority**

To configure the priority of the specified switch, use the `chassis priority` command.

```
chassis chassis-num priority chassis-priority
```

**Syntax Description**

- `chassis-num`  Chassis number is either 1 or 2.
- `chassis-priority`  Chassis priority value is either 1 or 2.

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to set the priority value to 2 for chassis number 1:

```
Device# chassis 1 priority 2
```
chassis timer peer-timeout

To configure chassis peer keepalive timeout value, use the `chassis timer peer-timeout` command.

```
chassis timer peer-timeout {timeout | default }
```

**Syntax Description**

- `timeout` Peer keepalive timeout value. Valid range is 500 to 16000 milliseconds.
- `default` Configures the default peer keepalive timeout value, which is 500 milliseconds.

**Command Default**

The default timeout is set to 500 milliseconds.

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You need not reload the device after executing this command. Also, this command configures both the devices at the same time with the same timeout value.

**Examples**

The following example shows how to set the chassis peer keepalive timeout value to the default value, which is 500 milliseconds:

```
Device# chassis timer peer-timeout default
```
class

To define a traffic classification match criteria for the specified class-map name, use the `class` command in policy-map configuration mode. Use the `no` form of this command to delete an existing class map.

```
class {class-map-name |class-default}
no class {class-map-name |class-default}
```

**Syntax Description**

- `class-map-name` The class map name.
- `class-default` Refers to a system default class that matches unclassified packets.

**Command Default**

No policy map class-maps are defined.

**Command Modes**

Policy-map configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Before using the `class` command, you must use the `policy-map` global configuration command to identify the policy map and enter policy-map configuration mode. After specifying a policy map, you can configure a policy for new classes or modify a policy for any existing classes in that policy map. You attach the policy map to a port by using the `service-policy` interface configuration command.

After entering the `class` command, you enter the policy-map class configuration mode. These configuration commands are available:

- `admit`—Admits a request for Call Admission Control (CAC)
- `bandwidth`—Specifies the bandwidth allocated to the class.
- `exit`—Exits the policy-map class configuration mode and returns to policy-map configuration mode.
- `no`—Returns a command to its default setting.
- `police`—Defines a policer or aggregate policer for the classified traffic. The policer specifies the bandwidth limitations and the action to take when the limits are exceeded. For more information about this command, see `Cisco IOS Quality of Service Solutions Command Reference` available on Cisco.com.
- `priority`—Assigns scheduling priority to a class of traffic belonging to a policy map.
- `queue-buffers`—Configures the queue buffer for the class.
- `queue-limit`—Specifies the maximum number of packets the queue can hold for a class policy configured in a policy map.
- `service-policy`—Configures a QoS service policy.
- `set`—Specifies a value to be assigned to the classified traffic. For more information, see `set`, on page 448
- `shape`—Specifies average or peak rate traffic shaping. For more information about this command, see `Cisco IOS Quality of Service Solutions Command Reference` available on Cisco.com.
To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

The **class** command performs the same function as the **class-map** global configuration command. Use the **class** command when a new classification, which is not shared with any other ports, is needed. Use the **class-map** command when the map is shared among many ports.

You can configure a default class by using the **class class-default** policy-map configuration command. Unclassified traffic (traffic that does not meet the match criteria specified in the traffic classes) is treated as default traffic.

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

**Examples**

This example shows how to create a policy map called policy1. When attached to the ingress direction, it matches all the incoming traffic defined in class1, sets the IP Differentiated Services Code Point (DSCP) to 10, and polices the traffic at an average rate of 1 Mb/s and bursts at 20 KB. Traffic exceeding the profile is marked down to a DSCP value gotten from the policed-DSCP map and then sent.

```
Device(config)# policy-map policy1
Device(config-pmap)# class class1
Device(config-pmap-c)# set dscp 10
Device(config-pmap-c)# police 1000000 20000 conform-action
Device(config-pmap-c)# police 1000000 20000 exceed-action
Device(config-pmap-c)# exit
```

This example shows how to configure a default traffic class to a policy map. It also shows how the default traffic class is automatically placed at the end of policy-map pm3 even though **class-default** was configured first:

```
Device# configure terminal
Device(config)# class-map cm-3
Device(config-cmap)# match ip dscp 30
Device(config-cmap)# exit

Device(config)# class-map cm-4
Device(config-cmap)# match ip dscp 40
Device(config-cmap)# exit

Device(config)# policy-map pm3
Device(config-pmap)# class class-default
Device(config-pmap-c)# set dscp 10
Device(config-pmap-c)# exit

Device(config-pmap)# class cm-3
Device(config-pmap-c)# set dscp 4
Device(config-pmap-c)# exit

Device(config-pmap)# class cm-4
Device(config-pmap-c)# set precedence 5
Device(config-pmap-c)# exit
Device(config-pmap)# exit

Device# show policy-map pm3
Policy Map pm3
Class cm-3
  set dscp 4
Class cm-4
  set precedence 5
```
Class class-default
   set dscp af11
classify

To classify a rule for rogue devices, use the `classify` command.

```plaintext
classify {friendly | malicious | delete}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>friendly</td>
<td>Classifies devices matching this rule as friendly.</td>
</tr>
<tr>
<td>malicious</td>
<td>Classifies devices matching this rule as malicious.</td>
</tr>
<tr>
<td>delete</td>
<td>Devices matching this rule are ignored.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

config-rule

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to classify rogue devices as friendly:

```plaintext
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless wps rogue rule my-rogue-rule priority 3
Device(config-rule)# classify friendly
```
class-map

To create a class map to be used for matching packets to the class whose name you specify and to enter class-map configuration mode, use the `class-map` command in global configuration mode. Use the `no` form of this command to delete an existing class map and to return to global or policy map configuration mode.

```plaintext
class-map [match-any] class-map-name
no class-map [match-any] class-map-name
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>match-any</td>
<td>(Optional) Perform a logical-OR of the matching statements under this class map. One or more criteria must be matched.</td>
</tr>
<tr>
<td>type</td>
<td>(Optional) Configures the CPL class map.</td>
</tr>
<tr>
<td>class-map-name</td>
<td>The class map name.</td>
</tr>
</tbody>
</table>

**Command Default**

No class maps are defined.

**Command Modes**

Global configuration

Policy map configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE 3.3SE</td>
<td>The <code>type</code> keyword was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to specify the name of the class for which you want to create or modify class-map match criteria and to enter class-map configuration mode.

The `class-map` command and its subcommands are used to define packet classification, marking, and aggregate policing as part of a globally named service policy applied on a per-port basis.

After you are in quality of service (QoS) class-map configuration mode, these configuration commands are available:

- `description`—Describes the class map (up to 200 characters). The `show class-map` privileged EXEC command displays the description and the name of the class map.
- `exit`—Exits from QoS class-map configuration mode.
- `match`—Configures classification criteria.
- `no`—Removes a match statement from a class map.

If you enter the `match-any` keyword, you can only use it to specify an extended named access control list (ACL) with the `match access-group` class-map configuration command.

To define packet classification on a physical-port basis, only one `match` command per class map is supported. The ACL can have multiple access control entries (ACEs).
Examples

This example shows how to configure the class map called class1 with one match criterion, which is an access list called 103:

```
Device(config)# access-list 103 permit ip any any dscp 10
Device(config)# class-map class1
Device(config-cmap)# match access-group 103
Device(config-cmap)# exit
```

This example shows how to delete the class map class1:

```
Device(config)# no class-map class1
```

You can verify your settings by entering the `show class-map` privileged EXEC command.
clear ip nbar protocol-discovery wlan

To clear the NBAR2 protocol discovery statistics on a specific WLAN, use the `clear ip nbar protocol-discovery wlan` command.

`clear ip nbar protocol-discovery wlan wlan-name`

**Syntax Description**

`wlan-name` Enter the WLAN name.

**Command Default**

None

**Command Modes**

Privileged EXEC

**Command History**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to clear the NBAR protocol discovery statistics on a particular WLAN:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# clear ip nbar protocol-discovery wlan wlan-name
```
clear platform condition all

To clear all conditional debug and packet-trace configuration and data, use the `clear platform condition all` command.

**clear platform condition all**

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>Privileged EXEC</td>
</tr>
<tr>
<td>Command History</td>
<td></td>
</tr>
<tr>
<td><strong>Release</strong></td>
<td><strong>Modification</strong></td>
</tr>
<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>

**Examples**

The following example shows how to clear all conditional debug and packet-trace configuration and data:

```
Device# clear platform condition all
```
clear subscriber policy peer

To clear the display of the details of a subscriber policy peer connection, use the `clear subscriber policy peer` command in privileged EXEC mode.

```
clear subscriber policy peer {address ip-address|handle connection-handle-id|session|all}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address</td>
<td>Clears the display of a specific peer connection, identified by its IP address.</td>
</tr>
<tr>
<td>ip-address</td>
<td>IP address of the peer connection to be cleared.</td>
</tr>
<tr>
<td>handle</td>
<td>Clears the display of a specific peer connection, identified by its handle.</td>
</tr>
<tr>
<td>connection-handle-id</td>
<td>Handle ID for the peer connection handle.</td>
</tr>
<tr>
<td>session</td>
<td>Clears the display of sessions with the given peer.</td>
</tr>
<tr>
<td>all</td>
<td>Clears the display of all peer connections.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SRC</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SB</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `clear subscriber policy peer` command ends the peering relationship between the Intelligent Services Gateway (ISG) device and selected Service Control Engine (SCE) devices. However, the SCE will attempt to reconnect with the ISG device after a configured amount of time. The `clear subscriber policy peer` command can remove select session associations from a particular SCE device.

**Examples**

The following example shows how the `clear subscriber policy peer` command is used at the router prompt to clear the display of all details of the subscriber policy peer connection.

```
Router# clear subscriber policy peer all
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show subscriber-policy peer</td>
<td>Displays the details of a subscriber policy peer.</td>
</tr>
<tr>
<td>subscriber-policy</td>
<td>Defines or modifies the forward and filter decisions of the subscriber policy.</td>
</tr>
</tbody>
</table>
client-access (mesh)

To configure backhaul with client access AP for a mesh AP profile, use the `client-access` command.

**client-access**

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

Backhaul client access is disabled.

**Command Modes**

`config-wireless-mesh-profile`

**Command History**

<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>

**Example**

The following example shows how to configure backhaul with client access AP for a mesh AP profile:

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

To configure the maximum number of client connections on a WLAN, use the `client association limit` command. To disable clients association limit on the WLAN, use the `no` form of this command.

```
client association limit {association-limit}
no client association limit {association-limit}
```

**Syntax Description**

- `association-limit`
  
  Number of client connections to be accepted. The range is from 0 to 2000. A value of zero (0) indicates no set limit.

**Command Default**

The maximum number of client connections is set to 0 (no limit).

**Command Modes**

WLAN configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE 3.3SE</td>
<td>The command was modified. The <code>ap</code> and <code>radio</code> keywords were added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

This example shows how to configure a client association limit on a WLAN and configure the client limit to 200:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# shutdown
Device(config-wlan)# client association limit 200
Device(config-wlan)# no shutdown
Device(config-wlan)# end
```

This example shows how to disable a client association limit on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# shutdown
Device(config-wlan)# no client association limit
Device(config-wlan)# no shutdown
Device(config-wlan)# end
```

This example shows how to configure a client association limit per radio on a WLAN and configure the client limit to 200:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan1
```
Device(config-wlan)# client association limit radio 200
Device(config-wlan)# no shutdown
Device(config-wlan)# end

This example shows how to configure a client association limit per AP on a WLAN and configure the client limit to 300:

Device(config)# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# client association limit ap 300
Device(config-wlan)# no shutdown
Device(config-wlan)# end
## channel foreign

To configure the RF Profile DCA foreign AP contribution, use the `channel foreign` command. To disable the DCA Foreign AP Contribution, use the `no` form of this command.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>foreign</td>
<td>Configures the RF Profile DCA foreign AP contribution.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

config-rf-profile

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Denali 16.3.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This example shows how to configure the RF profile DCA foreign AP contribution.

```
Device(config-rf-profile)#channel foreign
```
client-l2-vnid

To configure the client l2-vnid on a wireless fabric profile, use the client-l2-vnid command.

```
client-l2-vnid vnid
```

**Syntax Description**

- `vnid` Configures client l2-vnid. Valid range is 0 to 16777215.

**Command Default**

None

**Command Modes**

config-wireless-fabric

**Command History**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure the client l2-vnid value on a wireless fabric profile:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless profile fabric fabric-profile-name
Device(config-wireless-fabric)# client-l2-vnid 10
```
collect counter

To configure the number of bytes or packets in a flow as a non-key field for a flow record, use the **collect counter** command in flow record configuration mode. To disable the use of the number of bytes or packets in a flow (counters) as a non-key field for a flow record, use the **no** form of this command.

<table>
<thead>
<tr>
<th>Command Default</th>
<th>Command Modes</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td><strong>Release</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cisco IOS XE 3.2SE</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To return this command to its default settings, use the **no collect counter** or **default collect counter** flow record configuration command.

The following example configures the total number of bytes in the flows as a non-key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect counter bytes long
```

The following example configures the total number of packets from the flows as a non-key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect counter packets long
```
collect wireless ap mac address (wireless)

To enable the collection of MAC addresses of the access points that the wireless client is associated with, use the `collect wireless ap mac address` command in the flow record configuration mode. To disable the collection of access point MAC addresses, use the `no` form of this command.

`collect wireless ap mac address`
`no collect wireless ap mac address`

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

**Command Default**
The collection of access point MAC addresses is not enabled by default.

**Command Modes**
Flow record configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.3SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
The Flexible NetFlow `collect` commands are used to configure non-key fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in non-key fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a non-key field does not create a new flow. In most cases, the values for non-key fields are taken from only the first packet in the flow.

The following example configures the flow record to enable the collection of MAC addresses of the access points that the wireless client is associated with:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect wireless ap mac address
```
collect wireless client mac address (wireless)

To enable the collection of MAC addresses of the wireless clients that the access point is associated with, use the `collect wireless client mac address` command in the flow record configuration mode. To disable the collection of access point MAC addresses, use the `no` form of this command.

```
collect wireless client mac address
no collect wireless client mac address
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

The collection of wireless client MAC addresses is not enabled by default.

**Command Modes**

Flow record configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.3SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The Flexible NetFlow `collect` commands are used to configure non-key fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in non-key fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a non-key field does not create a new flow. In most cases, the values for non-key fields are taken from only the first packet in the flow.

The following example configures the flow record to enable the collection of MAC addresses of the access points that the wireless client is associated with:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect wireless client mac address
```
convergence

To configure mesh convergence method, use the convergence command.

```
convergence { fast | noise-tolerant-fast | standard | very-fast }
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fast</td>
<td>Configures fast convergence method.</td>
</tr>
<tr>
<td>noise-tolerant-fast</td>
<td>Configures noise-tolerant fast convergence method to handle unstable RF environment.</td>
</tr>
<tr>
<td>standard</td>
<td>Configures standard convergence method.</td>
</tr>
<tr>
<td>very-fast</td>
<td>Configures very fast convergence method.</td>
</tr>
</tbody>
</table>

**Command Default**

Standard

**Command Modes**

config-wireless-mesh-profile

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure the fast convergence method for a mesh AP profile:

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

To configure the voice and data coverage, use the **coverage** command. To reset the minimum RSSI value use the **no** form of this command.

**coverage {data | voice} rssi threshold value**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>data</th>
<th>Configure Coverage Hole Detection for data packets.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>voice</td>
<td>Configure Coverage Hole Detection for voice packets.</td>
</tr>
<tr>
<td></td>
<td>value</td>
<td>Minimum RSSI value for the packets received by the access point. The valid range is between –90 and –60 dBm.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

config-rf-profile

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Denali 16.3.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

None

This example shows how to configure the coverage hole detection for data packets.

```
Device(config-rf-profile)#coverage data rssi threshold -85
```
crypto key generate rsa

To generate Rivest, Shamir, and Adelman (RSA) key pairs, use the **crypto key generate rsa** command in global configuration mode.

```
crypto key generate rsa [ { general-keys | usage-keys | signature | encryption } ] [ label key-label ]
[ exportable ] [ modulus modulus-size ] [ storage devicename : ] [ redundancy ] [ on devicename : ]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>general-keys</td>
<td>(Optional) Specifies that a general-purpose key pair will be generated, which is the default.</td>
</tr>
<tr>
<td>usage-keys</td>
<td>(Optional) Specifies that two RSA special-usage key pairs, one encryption pair and one signature pair, will be generated.</td>
</tr>
<tr>
<td>signature</td>
<td>(Optional) Specifies that the RSA public key generated will be a signature special usage key.</td>
</tr>
<tr>
<td>encryption</td>
<td>(Optional) Specifies that the RSA public key generated will be an encryption special usage key.</td>
</tr>
</tbody>
</table>
| label key-label | (Optional) Specifies the name that is used for an RSA key pair when they are being exported.  
If a key label is not specified, the fully qualified domain name (FQDN) of the router is used. |
| exportable      | (Optional) Specifies that the RSA key pair can be exported to another Cisco device, such as a router. |
| modulus modulus-size | (Optional) Specifies the IP size of the key modulus.  
By default, the modulus of a certification authority (CA) key is 1024 bits. The recommended modulus for a CA key is 2048 bits. The range of a CA key modulus is from 350 to 4096 bits.  
**Note** Effective with Cisco IOS XE Release 2.4 and Cisco IOS Release 15.1(1)T, the maximum key size was expanded to 4096 bits for private key operations. The maximum for private key operations prior to these releases was 2048 bits. |
| storage devicename : | (Optional) Specifies the key storage location. The name of the storage device is followed by a colon (:). |
| redundancy      | (Optional) Specifies that the key should be synchronized to the standby CA. |
| on devicename : | (Optional) Specifies that the RSA key pair will be created on the specified device, including a Universal Serial Bus (USB) token, local disk, or NVRAM. The name of the device is followed by a colon (:).  
Keys created on a USB token must be 2048 bits or less. |

**Command Default**  
RSA key pairs do not exist.
### Command Modes

Global configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(8)T</td>
<td>The key-label argument was added.</td>
</tr>
<tr>
<td>12.2(15)T</td>
<td>The exportable keyword was added.</td>
</tr>
<tr>
<td>12.2(18)SXD</td>
<td>This command was integrated into Cisco IOS Release 12.2(18)SXD.</td>
</tr>
<tr>
<td>12.4(4)T</td>
<td>The storage keyword and devicename : argument were added.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>
| 12.4(11)T| The storage keyword and devicename : argument were implemented on the Cisco 7200VXR NPE-G2 platform.  
The signature, encryption and on keywords and devicename : argument were added. |
| 12.4(24)T| Support for IPv6 Secure Neighbor Discovery (SeND) was added. |
| XE 2.4  | The maximum RSA key size was expanded from 2048 to 4096 bits for private key operations. |
| 15.0(1)M| This command was modified. The redundancy keyword was introduced. |
| 15.1(1)T| This command was modified. The range value for the modulus keyword value is extended from 360 to 2048 bits to 360 to 4096 bits. |
| 15.2(2)SA2| This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches. |

### Usage Guidelines

**Note**

Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing.  
For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

Use this command to generate RSA key pairs for your Cisco device (such as a router).  
RSA keys are generated in pairs—one public RSA key and one private RSA key. 
If your router already has RSA keys when you issue this command, you will be warned and prompted to replace the existing keys with new keys.

**Note**

Before issuing this command, ensure that your router has a hostname and IP domain name configured (with the hostname and ip domain-name commands). You will be unable to complete the crypto key generate rsa command without a hostname and IP domain name. (This situation is not true when you generate only a named key pair.)
Secure Shell (SSH) may generate an additional RSA key pair if you generate a key pair on a router having no RSA keys. The additional key pair is used only by SSH and will have a name such as `{router_FQDN}.server`. For example, if a router name is “router1.cisco.com,” the key name is “router1.cisco.com.server.”

This command is not saved in the router configuration; however, the RSA keys generated by this command are saved in the private configuration in NVRAM (which is never displayed to the user or backed up to another device) the next time the configuration is written to NVRAM.

If the configuration is not saved to NVRAM, the generated keys are lost on the next reload of the router.

There are two mutually exclusive types of RSA key pairs: special-usage keys and general-purpose keys. When you generate RSA key pairs, you will be prompted to select either special-usage keys or general-purpose keys.

Special-Usage Keys

If you generate special-usage keys, two pairs of RSA keys will be generated. One pair will be used with any Internet Key Exchange (IKE) policy that specifies RSA signatures as the authentication method, and the other pair will be used with any IKE policy that specifies RSA encrypted keys as the authentication method.

A CA is used only with IKE policies specifying RSA signatures, not with IKE policies specifying RSA-encrypted nonces. (However, you could specify more than one IKE policy and have RSA signatures specified in one policy and RSA-encrypted nonces in another policy.)

If you plan to have both types of RSA authentication methods in your IKE policies, you may prefer to generate special-usage keys. With special-usage keys, each key is not unnecessarily exposed. (Without special-usage keys, one key is used for both authentication methods, increasing the exposure of that key.)

General-Purpose Keys

If you generate general-purpose keys, only one pair of RSA keys will be generated. This pair will be used with IKE policies specifying either RSA signatures or RSA encrypted keys. Therefore, a general-purpose key pair might get used more frequently than a special-usage key pair.

Named Key Pairs

If you generate a named key pair using the key-label argument, you must also specify the usage-keys keyword or the general-keys keyword. Named key pairs allow you to have multiple RSA key pairs, enabling the Cisco IOS software to maintain a different key pair for each identity certificate.

Modulus Length

When you generate RSA keys, you will be prompted to enter a modulus length. The longer the modulus, the stronger the security. However, a longer modulus takes longer to generate (see the table below for sample times) and takes longer to use.

**Table 7: Sample Times by Modulus Length to Generate RSA Keys**

<table>
<thead>
<tr>
<th>Router</th>
<th>360 bits</th>
<th>512 bits</th>
<th>1024 bits</th>
<th>2048 bits (maximum)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco 2500</td>
<td>11 seconds</td>
<td>20 seconds</td>
<td>4 minutes, 38 seconds</td>
<td>More than 1 hour</td>
</tr>
<tr>
<td>Cisco 4700</td>
<td>Less than 1 second</td>
<td>1 second</td>
<td>4 seconds</td>
<td>50 seconds</td>
</tr>
</tbody>
</table>
Cisco IOS software does not support a modulus greater than 4096 bits. A length of less than 512 bits is normally not recommended. In certain situations, the shorter modulus may not function properly with IKE, so we recommend using a minimum modulus of 2048 bits.

**Note**
As of Cisco IOS Release 12.4(11)T, peer public RSA key modulus values up to 4096 bits are automatically supported. The largest private RSA key modulus is 4096 bits. Therefore, the largest RSA private key a router may generate or import is 4096 bits. However, RFC 2409 restricts the private key size to 2048 bits or less for RSA encryption. The recommended modulus for a CA is 2048 bits; the recommended modulus for a client is 2048 bits.

Additional limitations may apply when RSA keys are generated by cryptographic hardware. For example, when RSA keys are generated by the Cisco VPN Services Port Adapter (VSPA), the RSA key modulus must be a minimum of 384 bits and must be a multiple of 64.

**Specifying a Storage Location for RSA Keys**

When you issue the `crypto key generate rsa` command with the `storage devicename :` keyword and argument, the RSA keys will be stored on the specified device. This location will supersede any `crypto key storage` command settings.

**Specifying a Device for RSA Key Generation**

As of Cisco IOS Release 12.4(11)T and later releases, you may specify the device where RSA keys are generated. Devices supported include NVRAM, local disks, and USB tokens. If your router has a USB token configured and available, the USB token can be used as cryptographic device in addition to a storage device. Using a USB token as a cryptographic device allows RSA operations such as key generation, signing, and authentication of credentials to be performed on the token. The private key never leaves the USB token and is not exportable. The public key is exportable.

RSA keys may be generated on a configured and available USB token, by the use of the `on devicename :` keyword and argument. Keys that reside on a USB token are saved to persistent token storage when they are generated. The number of keys that can be generated on a USB token is limited by the space available. If you attempt to generate keys on a USB token and it is full you will receive the following message:

```
% Error in generating keys: no available resources
```

Key deletion will remove the keys stored on the token from persistent storage immediately. (Keys that do not reside on a token are saved to or deleted from nontoken storage locations when the `copy` or similar command is issued.)


**Specifying RSA Key Redundancy Generation on a Device**

You can specify redundancy for existing keys only if they are exportable.

**Examples**

The following example generates a general-usage 1024-bit RSA key pair on a USB token with the label “ms2” with crypto engine debugging messages shown:

```
Router(config)# crypto key generate rsa label ms2 modulus 2048 on usbtoken0:
```
The name for the keys will be: ms2
% The key modulus size is 2048 bits
% Generating 1024 bit RSA keys, keys will be on-token, non-exportable...
Jan 7 02:41:40.895: crypto_engine: Generate public/private keypair [OK]
Jan 7 02:44:09.623: crypto_engine: Create signature
Jan 7 02:44:10.467: crypto_engine: Verify signature
Jan 7 02:44:10.467: CryptoEngine0: CRYPTO_ISA_RSA_CREATE_PUBKEY(hw)(ipsec)
Jan 7 02:44:10.467: CryptoEngine0: CRYPTO_ISA_RSA_PUB_DECRYPT(hw)(ipsec)

Now, the on-token keys labeled “ms2” may be used for enrollment.

The following example generates special-usage RSA keys:

Router(config)# crypto key generate rsa usage-keys
The name for the keys will be: myrouter.example.com
Choose the size of the key modulus in the range of 360 to 2048 for your Signature Keys.
Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus[512]? <return>
Generating RSA keys.... [OK].
Choose the size of the key modulus in the range of 360 to 2048 for your Encryption Keys.
Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus[512]? <return>
Generating RSA keys.... [OK].

The following example generates general-purpose RSA keys:

Note
You cannot generate both special-usage and general-purpose keys; you can generate only one or the other.

Router(config)# crypto key generate rsa general-keys
The name for the keys will be: myrouter.example.com
Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus[512]? <return>
Generating RSA keys.... [OK].

The following example generates the general-purpose RSA key pair “exampleCAkeys”:

crypto key generate rsa general-keys label exampleCAkeys
crypto ca trustpoint exampleCAkeys
enroll url
http://exampleCAkeys/certsrv/mscep/mscep.dll
rsakeypair exampleCAkeys 1024 1024

The following example specifies the RSA key storage location of “usbtoken0:” for “tokenkey1”:
crypto key generate rsa general-keys label tokenkey1 storage usbtoken0:

The following example specifies the redundancy keyword:

Router(config)# crypto key generate rsa label MYKEYS redundancy
The name for the keys will be: MYKEYS
Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]:

% Generating 512 bit RSA keys, keys will be non-exportable with redundancy...[OK]

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>copy</td>
<td>Copies any file from a source to a destination, use the copy command in privileged EXEC mode.</td>
<td></td>
</tr>
<tr>
<td>crypto key storage</td>
<td>Sets the default storage location for RSA key pairs.</td>
<td></td>
</tr>
<tr>
<td>debug crypto engine</td>
<td>Displays debug messages about crypto engines.</td>
<td></td>
</tr>
<tr>
<td>hostname</td>
<td>Specifies or modifies the hostname for the network server.</td>
<td></td>
</tr>
<tr>
<td>ip domain-name</td>
<td>Defines a default domain name to complete unqualified hostnames (names without a dotted-decimal domain name).</td>
<td></td>
</tr>
<tr>
<td>show crypto key mypubkey rsa</td>
<td>Displays the RSA public keys of your router.</td>
<td></td>
</tr>
<tr>
<td>show crypto pki certificates</td>
<td>Displays information about your PKI certificate, certification authority, and any registration authority certificates.</td>
<td></td>
</tr>
</tbody>
</table>
cts inline-tagging

To configure Cisco TrustSec (CTS) inline tagging, use the cts inline-tagging command.

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

Inline tagging is not configured.

**Command Modes**

wireless policy configuration (config-wireless-policy)

**Command History**

<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>

**Example**

This example shows how to configure CTS inline tagging.

Device(config-wireless-policy)# cts inline-tagging
cts role-based enforcement

To configure Cisco TrustSec (CTS) SGACL enforcement, use the cts role-based enforcement command.

Syntax Description

This command has no keywords or arguments.

Command Default

SGACL is not enforced.

Command Modes

wireless policy configuration (config-wireless-policy)

Command History

<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>

Example

This example shows how to configure CTS SGACL enforcement.

Device(config-wireless-policy)# cts role-based enforcement
To set the Cisco TrustSec (CTS) default security group tag (SGT), use the `cts sgt` command.

```
cts sgt  sgt-value
```

**Syntax Description**

| sgt-value | Security group tag value.
|

**Command Default**

SGT tag is not set.

**Command Modes**

wireless policy configuration (config-wireless-policy)

**Command History**

<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>

**Example**

This example shows how to set the default SGT.

```
Device(config-wireless-policy)# cts sgt 100
```
custom-page login device

To configure a customized login page, use the custom-page login device command.

```
custom-page login device html-filename
```

**Syntax Description**
- `html-filename` Enter the HTML filename of the login page.

**Command Default**
None

**Command Modes**
config-params-parameter-map

**Command History**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure a customized login page:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# parameter-map type webauth parameter-map-name
Device(config-params-parameter-map)# custom-page login device bootflash:login.html
```
default

To set the parameters to their default values, use the `default` command.

```
default { aaa-override | accounting-list | band-select | broadcast-ssid | call-snoop | ccx | channel-scan | parameters | chd | client | datalink | diag-channel | dtim | exclusionlist | ip | ipv6 | load-balance | local-auth | mac-filtering | media-stream | mfp }
```

**Syntax Description**

- **aaa-override**
  Sets the AAA override parameter to its default value.

- **accounting-list**
  Sets the accounting parameter and its attributes to their default values.

- **band-select**
  Sets the band selection parameter to its default values.

- **broadcast-ssid**
  Sets the broadcast Service Set Identifier (SSID) parameter to its default value.

- **call-snoop**
  Sets the call snoop parameter to its default value.

- **ccx**
  Sets the Cisco client extension (Cisco Aironet IE) parameters and attributes to their default values.

- **channel-scan**
  Sets the channel scan parameters and attributes to their default values.

- **chd**
  Sets the coverage hold detection parameter to its default value.

- **client**
  Sets the client parameters and attributes to their default values.

- **datalink**
  Sets the datalink parameters and attributes to their default values.

- **diag-channel**
  Sets the diagnostic channel parameters and attributes to their default values.

- **dtim**
  Sets the Delivery Traffic Indicator Message (DTIM) parameter to its default value.

- **exclusionlist**
  Sets the client exclusion timeout parameter to its default value.

- **ip**
  Sets the IP parameters to their default values.

- **ipv6**
  Sets the IPv6 parameters and attributes to their default values.

- **load-balance**
  Sets the load-balancing parameter to its default value.

- **local-auth**
  Sets the Extensible Authentication Protocol (EAP) profile parameters and attributes to their default values.

- **mac-filtering**
  Sets the MAC filtering parameters and attributes to their default values.

- **media-stream**
  Sets the media stream parameters and attributes to their default values.

- **mfp**
  Sets the Management Frame Protection (MPF) parameters and attributes to their default values.
### Command: default

Sets the mobility parameters and attributes to their default values.

Sets the RADIUS Network Admission Control (NAC) parameter to its default value.

Sets the passive client parameter to its default value.

Sets the peer to peer blocking parameters and attributes to their default values.

Sets the radio policy parameters and attributes to their default values.

Sets the roamed voice client parameters and attributes to their default values.

Sets the security policy parameters and attributes to their default values.

Sets the WLAN quality of service (QoS) policy parameters and attributes to their default values.

Sets the client session timeout parameter to its default value.

Sets the shutdown parameter to its default value.

Sets the Session Initiation Protocol (SIP) Call Admission Control (CAC) parameters and attributes to their default values.

Sets the static IP client tunneling parameters and their attributes to their default values.

Sets the Wi-Fi Multimedia (WMM) Unscheduled Automatic Power Save Delivery (UAPSD) parameters and attributes to their default values.

Sets the Workgroup Bridges (WGB) parameter to its default value.

Sets the WMM parameters and attributes to their default values.

### Command Default

None.

### Command Modes

WLAN configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

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

This example shows how to set the Cisco Client Extension parameter to its default value:

```bash
Device(config-wlan)# default ccx aironet-iesupport
```
### debug platform qos-acl-tcam

To enable debugging of the quality of service (QoS) and access control list (ACL) hardware memory manager software, use the `debug platform qos-acl-tcam` command in privileged or user EXEC mode. To disable debugging, use the `no` form of this command.

```
 debug platform qos-acl-tcam { all | ctcam | errors | labels | mask | rpc | tcam }
 no debug platform qos-acl-tcam { all | ctcam | errors | labels | mask | rpc | tcam }
```

#### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Displays all QoS and ACL ternary content addressable memory (QATM) manager debug messages.</td>
</tr>
<tr>
<td>ctcam</td>
<td>Displays Cisco TCAM (CTCAM) related-events debug messages.</td>
</tr>
<tr>
<td>errors</td>
<td>Displays QATM error-related-events debug messages.</td>
</tr>
<tr>
<td>labels</td>
<td>Displays QATM label-related-events debug messages.</td>
</tr>
<tr>
<td>mask</td>
<td>Displays QATM mask-related-events debug messages.</td>
</tr>
<tr>
<td>rpc</td>
<td>Displays QATM remote procedure call (RPC) related-events debug messages.</td>
</tr>
<tr>
<td>tcam</td>
<td>Displays QATM hardware-memory-related events debug messages.</td>
</tr>
</tbody>
</table>

#### Command Default

Debugging is disabled.

#### Command Modes

User EXEC

Privileged EXEC

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

The `undebug platform qos-acl-tcam` command is the same as the `no debug platform qos-acl-tcam` command.

When you enable debugging on a switch stack, it is enabled only on the active switch. To enable debugging on a stack member, you can start a session from the active switch by using the `session switch-number` EXEC command. Then enter the `debug` command at the command-line prompt of the stack member. You also can use the `remote command` `stack-member-number LINE` EXEC command on the active switch to enable debugging on a member switch without first starting a session.
debug qos-manager

To enable debugging of the quality of service (QoS) manager software, use the `debug qos-manager` command in privileged EXEC mode. Use the `no` form of this command to disable debugging.

```
debug qos-manager {all|event|verbose}
no debug qos-manager {all|event|verbose}
```

**Syntax Description**

- **all**: Display all QoS-manager debug messages.
- **event**: Display QoS-manager related-event debug messages.
- **verbose**: Display QoS-manager detailed debug messages.

**Command Default**

Debugging is disabled.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `undebug qos-manager` command is the same as the `no debug qos-manager` command.
To configure a description for a flow monitor, flow exporter, or flow record, use the `description` command in the appropriate configuration mode. To remove a description, use the `no` form of this command.

```
description  description
no description  description
```

**Syntax Description**
- `description` Text string that describes the flow monitor, flow exporter, or flow record.

**Command Default**
The default description for a flow sampler, flow monitor, flow exporter, or flow record is "User defined."

**Command Modes**
The following command modes are supported:
- Flow exporter configuration
- Flow monitor configuration
- Flow record configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
To return this command to its default setting, use the `no description` or `default description` command in the appropriate configuration mode.

The following example configures a description for a flow monitor:

```
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)# description Monitors traffic to 172.16.0.1 255.255.0.0
```
destination

To configure an export destination for a flow exporter, use the `destination` command in flow exporter configuration mode. To remove an export destination for a flow exporter, use the `no` form of this command.

```
destination {hostname|ip-address}
no destination {hostname|ip-address}
```

**Syntax Description**

- `hostname` Hostname of the device to which you want to send the NetFlow information.
- `ip-address` IPv4 address of the workstation to which you want to send the NetFlow information.

**Command Default**

An export destination is not configured.

**Command Modes**

Flow exporter configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Each flow exporter can have only one destination address or hostname.

When you configure a hostname instead of the IP address for the device, the hostname is resolved immediately and the IPv4 address is stored in the running configuration. If the hostname-to-IP-address mapping that was used for the original Domain Name System (DNS) name resolution changes dynamically on the DNS server, the device does not detect this, and the exported data continues to be sent to the original IP address, resulting in a loss of data.

To return this command to its default setting, use the `no destination` or `default destination` command in flow exporter configuration mode.

The following example shows how to configure the networking device to export the cache entry to a destination system:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# destination 10.0.0.4
```
device-role (IPv6 snooping)

To specify the role of the device attached to the port, use the `device-role` command in IPv6 snooping configuration mode.

```
device-role  { node | switch }
```

**Syntax Description**
- `node` Sets the role of the attached device to node.
- `switch` Sets the role of the attached device to switch.

**Command Default**
The device role is node.

**Command Modes**
IPv6 snooping configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
The `device-role` command specifies the role of the device attached to the port. By default, the device role is node.

The `switch` keyword indicates that the remote device is a switch and that the local switch is now operating in multiswitch mode; binding entries learned from the port will be marked with trunk_port preference level. If the port is configured as a trust-port, binding entries will be marked with trunk_trusted_port preference level.

This example shows how to define an IPv6 snooping policy name as policy1, place the device in IPv6 snooping configuration mode, and configure the device as the node:

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# device-role node
```
device-role (IPv6 nd inspection)

To specify the role of the device attached to the port, use the `device-role` command in neighbor discovery (ND) inspection policy configuration mode.

```
device-role { host | monitor | router | switch }
```

**Syntax Description**
- **host**: Sets the role of the attached device to host.
- **monitor**: Sets the role of the attached device to monitor.
- **router**: Sets the role of the attached device to router.
- **switch**: Sets the role of the attached device to switch.

**Command Default**
The device role is host.

**Command Modes**
ND inspection policy configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Denali 16.3.1</td>
<td>The keywords <code>monitor</code> and <code>router</code> are deprecated.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
The `device-role` command specifies the role of the device attached to the port. By default, the device role is host, and therefore all the inbound router advertisement and redirect messages are blocked. If the device role is enabled using the `router` keyword, all messages (router solicitation [RS], router advertisement [RA], or redirect) are allowed on this port.

When the `router` or `monitor` keyword is used, the multicast RS messages are bridged on the port, regardless of whether limited broadcast is enabled. However, the monitor keyword does not allow inbound RA or redirect messages. When the monitor keyword is used, devices that need these messages will receive them.

The `switch` keyword indicates that the remote device is a switch and that the local switch is now operating in multiswitch mode; binding entries learned from the port will be marked with `trunk_port` preference level. If the port is configured as a trust-port, binding entries will be marked with `trunk_trusted_port` preference level.

The following example defines a Neighbor Discovery Protocol (NDP) policy name as policy1, places the device in ND inspection policy configuration mode, and configures the device as the host:

```
Device(config)# ipv6 nd inspection policy policy1
Device(config-nd-inspection)# device-role host
```
device-tracking binding vlan

To configure IPv4 or IPv6 static entry, use the `device-tracking binding vlan` command.

```
device-tracking binding vlan vlan-id {ipv4-addr ipv6-addr} interface gigabitEthernet ge-intf-num hardware-or-mac-address
```

**Syntax Description**

- **vlan-id**: VLAN ID. Valid range is 1 to 4096.
- **ipv4-addr**: IPv4 address of the device.
- **ipv6-addr**: IPv6 address of the device.
- **interface gigabitEthernet**: GigabitEthernet IEEE 802.3z.
- **ge-intf-num**: GigabitEthernet interface number. Valid range is 1 to 32.
- **hardware-or-mac-address**: The 48-bit hardware address or the MAC address of the device.

**Command Default**

None

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
</table>
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

**Examples**

The following example shows how to configure IPv4 static entry:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# device-tracking binding vlan 20 20.20.20.5 interface gigabitEthernet 1 0000.1111.2222
```
device-tracking policy

To configure a Switch Integrated Security Features (SISF)-based IP device tracking policy, use the `device-tracking` command in global configuration mode. To delete a device tracking policy, use the `no` form of this command.

```
device-tracking policy  policy-name
no device-tracking policy  policy-name
```

**Syntax Description**

- `policy-name` User-defined name of the device tracking policy. The policy name can be a symbolic string (such as Engineering) or an integer (such as 0).

**Command Default**

A device tracking policy is not configured.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Denali 16.1.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the SISF-based `device-tracking policy` command to create a device tracking policy. When the `device-tracking policy` command is enabled, the configuration mode changes to device-tracking configuration mode. In this mode, the administrator can configure the following first-hop security commands:

- (Optional) `device-role {node | switch}`—Specifies the role of the device attached to the port. Default is `node`.
- (Optional) `limit address-count value`—Limits the number of addresses allowed per target.
- (Optional) `no`—Negates a command or sets it to defaults.
- (Optional) `destination-glean {recovery | log-only} [dhcp]`—Enables binding table recovery by data traffic source address gleaning.
- (Optional) `data-glean {recovery | log-only} [dhcp | ndp]`—Enables binding table recovery using source or data address gleaning.
- (Optional) `security-level {glean | guard | inspect}`—Specifies the level of security enforced by the feature. Default is `guard`.
  - `glean`—Gleans addresses from messages and populates the binding table without any verification.
  - `guard`—Gleans addresses and inspects messages. In addition, it rejects RA and DHCP server messages. This is the default option.
  - `inspect`—Gleans addresses, validates messages for consistency and conformance, and enforces address ownership.
- (Optional) `tracking {disable | enable}`—Specifies a tracking option.
- (Optional) `trusted-port`—Sets up a trusted port. It disables the guard on applicable targets. Bindings learned through a trusted port have preference over bindings learned through any other port. A trusted port is given preference in case of a collision while making an entry in the table.
This example shows how to configure an a device-tracking policy:

```
Device(config)# device-tracking policy policy1
Device(config-device-tracking)# trusted-port
```
To configure DHCP TLV caching on a WLAN, use the `dhcp-tlv-caching` command.

**Example**

This example shows how to configure DHCP TLV caching on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless profile policy rr-xyz-policy-1
Device(config-wireless-policy)# dhcp-tlv-caching
Device(config-wireless-policy)# radius-profiling
Device(config-wireless-policy)# end
```
**dns-server (IPv6)**

To specify the Domain Name System (DNS) IPv6 servers available to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the `dns-server` command in DHCP for IPv6 pool configuration mode. To remove the DNS server list, use the `no` form of this command.

```
dns-server ipv6-address
no dns-server ipv6-address
```

**Syntax Description**

<table>
<thead>
<tr>
<th><code>ipv6-address</code></th>
<th>The IPv6 address of a DNS server.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.</td>
</tr>
</tbody>
</table>

**Command Default**

When a DHCP for IPv6 pool is first created, no DNS IPv6 servers are configured.

**Command Modes**

DHCP for IPv6 pool configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(4)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was integrated into Cisco IOS XE Release 2.1.</td>
</tr>
<tr>
<td>12.2(33)SRE</td>
<td>This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.</td>
</tr>
<tr>
<td>12.2(33)XNE</td>
<td>This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Multiple Domain Name System (DNS) server addresses can be configured by issuing this command multiple times. New addresses will not overwrite old addresses.

**Examples**

The following example specifies the DNS IPv6 servers available:

```
dns-server 2001:0DB8:3000:0000::42
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain-name</td>
<td>Configures a domain name for a DHCP for IPv6 client.</td>
</tr>
<tr>
<td>ipv6 dhcp pool</td>
<td>Configures a DHCP for IPv6 configuration information pool and enters DHCP for IPv6 pool configuration mode.</td>
</tr>
</tbody>
</table>
To enable or disable DNScrypt, use the `dnscrypt` command.

```
dnscrypt
```

**Command Default**
None

**Command Modes**
config-profile

**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>

**Usage Guidelines**
By default, the DNScrypt option is enabled.

This example shows how to enable or disable DNScrypt:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# parameter-map type umbrella global
Device(config-profile)# token 57CC80106C087FB1B2A7BAB4F2F4373C00247166
Device(config-profile)# local-domain dns_wl
Device(config-profile)# no dnscrypt
Device(config-profile)# end
```
To specify the domain name for a Dynamic Host Configuration Protocol (DHCP) client, use the `domain-name` command in DHCP pool configuration mode. To remove the domain name, use the `no` form of this command.

```
domain-name domain
no domain-name
```

**Syntax Description**

```
domain | Specifies the domain name string of the client.
```

**Command Default**

No default behavior or values.

**Command Modes**

DHCP pool configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(1)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Examples**

The following example specifies cisco.com as the domain name of the client:

```
domain-name cisco.com
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dns-server</code></td>
<td>Specifies the DNS IP servers available to a DHCP client.</td>
</tr>
<tr>
<td><code>ip dhcp pool</code></td>
<td>Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.</td>
</tr>
</tbody>
</table>
dot11 airtime-fairness

To configure airtime-fairness policy for 2.4- or 5-GHz radio, use the dot11 airtime-fairness command.

```
dot11 {24ghz | 5ghz} airtime-fairness atf-policy-name
```

**Syntax Description**

- `atf-policy-name`: Is the name of the airtime-fairness policy.

**Command Default**

None

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>3.2SE</td>
<td></td>
</tr>
</tbody>
</table>

This example shows how to configure airtime-fairness policy for 2.4- or 5-GHz radio:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless profile policy <profile-name>
Device(config-wireless-policy)# dot11 24ghz airtime-fairness <atf-policy-name>
Device(config-wireless-policy)# end
```
**dot11 5ghz reporting-interval**

To configure the client report interval sent from AP for clients on 802.11a radio, use the `dot11 5ghz reporting-interval` command.

**Syntax Description**

- `reporting-interval` Interval at which client report needs to be sent in seconds.

**Command Default**

None

**Command Modes**

- config-ap-profile

**Command History**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to set the client report interval in seconds:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# ap profile profile-name
Device(config-ap-profile)# dot11 5ghz reporting-interval 8
```
**dot11 reporting-interval**

To set the volume metering interval, use the `dot11 reporting-interval` command.

```
dot11 {24ghz | 5ghz} reporting-interval
```

**Syntax Description**

- `reporting-interval` Interval to send client accounting statistics.

**Command Default**

Interval is configured at the default level of 90 seconds.

**Command Modes**

- `config-ap-profile`

**Command History**

<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>

**Usage Guidelines**

Though the CLI allows you to configure range from 5 to 90 seconds, we recommend that you use 60 to 90 seconds range for Volume Metering.

This CLI can also be used to configure the interval when smart roam is enabled, which has a range of 5 to 90 seconds.

Though you can set two different values for volume metering and smart roam, only one value takes effect based on the order of execution. So, we recommend that you use the same reporting interval for both.

**Example**

The following example shows how to configure volume metering:

```
Device(config-ap-profile)# dot11 24ghz 60
```
**dot1x system-auth-control**

To globally enable 802.1X SystemAuthControl (port-based authentication), use the `dot1x system-auth-control` command in global configuration mode. To disable SystemAuthControl, use the `no` form of this command.

```
dot1x system-auth-control
no dot1x system-auth-control
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

System authentication is disabled by default. If this command is disabled, all ports behave as if they are force authorized.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(2)XA</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(14)SX</td>
<td>This command was implemented on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was integrated into Cisco IOS Release 12.3(4)T.</td>
</tr>
<tr>
<td>12.2(17d)SX B</td>
<td>Support for this command on the Supervisor Engine 2 was extended to 12.2(17d)SX B.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SX H</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SX H.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The IEEE 802.1x standard defines a client-server-based access control and authentication protocol that restricts unauthorized devices from connecting to a LAN through publicly accessible ports. 802.1x controls network access by creating two distinct virtual access points at each port. One access point is an uncontrolled port; the other is a controlled port. All traffic through the single port is available to both access points. 802.1x authenticates each user device that is connected to a switch port and assigns the port to a VLAN before making available any services that are offered by the switch or the LAN. Until the device is authenticated, 802.1x access control allows only Extensible Authentication Protocol (EAP) over LAN (EAPOL) traffic through the port to which the device is connected. After authentication is successful, normal traffic can pass through the port.

The `no` form of the command removes any 802.1X-related configurations.

**Catalyst 6500 Series Switch and Cisco 7600 Series**

You must enable Authentication, Authorization, and Accounting (AAA) and specify the authentication method list before enabling 802.1X. A method list describes the sequence and authentication methods to be queried to authenticate a user.

**Examples**

The following example shows how to enable SystemAuthControl:
Router(config)# dot1x system-auth-control

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>aaa authentication dot1x</td>
<td>Specifies one or more AAA methods for use on interfaces running IEEE 802.1X.</td>
</tr>
<tr>
<td></td>
<td>aaa new-model</td>
<td>Enables the AAA access-control model.</td>
</tr>
<tr>
<td></td>
<td>debug dot1x</td>
<td>Displays 802.1X debugging information.</td>
</tr>
<tr>
<td></td>
<td>description</td>
<td>Specifies a description for an 802.1X profile.</td>
</tr>
<tr>
<td></td>
<td>device</td>
<td>Statically authorizes or rejects individual devices.</td>
</tr>
<tr>
<td></td>
<td>dot1x initialize</td>
<td>Initializes 802.1X state machines on all 802.1X-enabled interfaces.</td>
</tr>
<tr>
<td></td>
<td>dot1x max-req</td>
<td>Sets the maximum number of times that a router or Ethernet switch network module can send an EAP request/identity frame to a client (assuming that a response is not received) before restarting the authentication process.</td>
</tr>
<tr>
<td></td>
<td>dot1x port-control</td>
<td>Enables manual control of the authorized state of a controlled port.</td>
</tr>
<tr>
<td></td>
<td>dot1x re-authenticate</td>
<td>Manually initiates a reauthentication of the specified 802.1X-enabled ports.</td>
</tr>
<tr>
<td></td>
<td>dot1x reauthentication</td>
<td>Globally enables periodic reauthentication of the client PCs on the 802.1X interface.</td>
</tr>
<tr>
<td></td>
<td>dot1x timeout</td>
<td>Sets retry timeouts.</td>
</tr>
<tr>
<td></td>
<td>identity profile</td>
<td>Creates an identity profile and enters identity profile configuration mode.</td>
</tr>
<tr>
<td></td>
<td>show dot1x</td>
<td>Displays details and statistics for an identity profile.</td>
</tr>
<tr>
<td></td>
<td>template</td>
<td>Specifies a virtual template from which commands may be cloned.</td>
</tr>
</tbody>
</table>
To configure an EAP profile, use the `eap profile` command.

```
  eap profile  profile-name
```

**Syntax Description**
- `profile-name`  Name of the EAP profile. Maximum number of allowed characters is 63.

**Command Default**
- None

**Command Modes**
- Global configuration (config)

**Command History**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure an EAP profile name:

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

To enable Encrypted Traffic Analytics (ETA) globally on Cisco Elastic Wireless LAN Controller (eWLC), use the `et-analytics` command.

**et-analytics**

**Command Default**

None

**Command Modes**

ET-Analytics configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>3.2SE</td>
<td></td>
</tr>
</tbody>
</table>

This example shows how to enable Encrypted Traffic Analytics (ETA) globally on Cisco Elastic Wireless LAN Controller (eWLC) in the ET-Analytics configuration mode:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# et-analytics
Device(config-et-analytics)# end
```
ethernet-vlan-transparent (mesh)

To configure ethernet bridging VLAN transparency for a mesh AP profile, use the `ethernet-vlan-transparent` command.

**ethernet-vlan-transparent**

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

**Command Default**
Ethernet bridging VLAN transparency is enabled.

**Command Modes**
config-wireless-mesh-profile

**Command History**

<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>

**Example**
The following example shows how to configure ethernet bridging VLAN transparency for a mesh AP profile:

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

To configure ethernet bridging for a mesh AP profile, use the `ethernet-bridging` command.

**ethernet-bridging**

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

**Command Default**
Ethernet bridging is disabled.

**Command Modes**
config-wireless-mesh-profile

**Command History**

<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>

**Example**

The following example shows how to configure ethernet bridging for a mesh AP profile:

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

To specify the match criteria to a policy map, use the **event identity-update** command.

```
event identity-update [{match-all | match-first}]
```

**Syntax Description**

- **match-all** Evaluates all the classes.
- **match-first** Evaluates the first class.

**Command Default**
None

**Command Modes**
config-event-control-policymap

**Command History**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to specify the match criteria as match all classes to a policy map:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# policy-map type control subscriber policy-map-name
Device(config-event-control-policymap)# event identity-update match-all
```
To configure an exclusion list on a wireless LAN, use the `exclusionlist` command. To disable an exclusion list, use the `no` form of this command.

```
exclusionlist [timeout seconds]
no exclusionlist [timeout]
```

**Syntax Description**
- `timeout seconds` (Optional) Specifies an exclusion list timeout in seconds. The range is from 0 to 2147483647. A value of zero (0) specifies no timeout.

**Command Default**
The exclusion list is set to 60 seconds.

**Command Modes**
WLAN configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>3.2SE</td>
<td></td>
</tr>
</tbody>
</table>

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

This example shows how to configure a client exclusion list for a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# exclusionlist timeout 345
```

This example shows how to disable a client exclusion list on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no exclusionlist timeout 345
```
fabric control-plane

To configure the fabric control plane details, use the `fabric control-plane` command.

```
fabric control-plane  map-server-name
```

**Syntax Description**

- `map-server-name` Refers to the fabric control plane name associated with the site tag.

**Command Default**

None

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

This example shows how to configure the fabric control plane details:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless tag site default-site-tag
Device(config-site-tag)# fabric control-plane
map-server-name
Device(config-site-tag)# end
```
fallback-radio-shut

To configure shutdown of the radio interface, use the `fallback-radio-shut` command.

**fallback-radio-shut**

<table>
<thead>
<tr>
<th>Command Default</th>
<th>Command Modes</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>config-wireless-flex-profile</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Release</strong></td>
</tr>
<tr>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure shutdown of the radio interface:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless profile flex flex-profile-name
Device(config-wireless-flex-profile)# fallback-radio-shut
```
To configure flex related parameters, use the `flex` command.

```
flex {nat-pat | split-mac-acl split-mac-acl-name | vlan-central-switching }
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>nat-pat</td>
<td>Enables NAT-PAT.</td>
</tr>
<tr>
<td>split-mac-acl</td>
<td>Configures split-mac-acl name.</td>
</tr>
<tr>
<td>split-mac-acl-name</td>
<td>Name of split MAC ACL.</td>
</tr>
<tr>
<td>vlan-central-switching</td>
<td>VLAN based central switching.</td>
</tr>
</tbody>
</table>

**Command Default**
None

**Command Modes**
config-wireless-policy

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to configure flex related VLAN central-switching:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless profile policy profile-name
Device(config-wireless-policy)# flex vlan-central-switching
```
flow exporter

To create a flow exporter, or to modify an existing flow exporter, and enter flow exporter configuration mode, use the `flow exporter` command in global configuration mode. To remove a flow exporter, use the `no` form of this command.

```
flow exporter exporter-name
no flow exporter exporter-name
```

**Syntax Description**

- `exporter-name` Name of the flow exporter that is being created or modified.

**Command Default**

Flow exporters are not present in the configuration.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Flow exporters export the data in the flow monitor cache to a remote system, such as a server running NetFlow collector, for analysis and storage. Flow exporters are created as separate entities in the configuration. Flow exporters are assigned to flow monitors to provide data export capability for the flow monitors. You can create several flow exporters and assign them to one or more flow monitors to provide several export destinations. You can create one flow exporter and apply it to several flow monitors.

**Examples**

The following example creates a flow exporter named FLOW-EXPORTER-1 and enters flow exporter configuration mode:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)#
```
flow monitor

To create a flow monitor, or to modify an existing flow monitor, and enter flow monitor configuration mode, use the `flow monitor` command in global configuration mode. To remove a flow monitor, use the `no` form of this command.

```
flow monitor monitor-name
no flow monitor monitor-name
```

**Syntax Description**

- `monitor-name` Name of the flow monitor that is being created or modified.

**Command Default**

Flow monitors are not present in the configuration.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Flow monitors are the component that is applied to interfaces to perform network traffic monitoring. Flow monitors consist of a flow record and a cache. You add the record to the flow monitor after you create the flow monitor. The flow monitor cache is automatically created at the time the flow monitor is applied to the first interface. Flow data is collected from the network traffic during the monitoring process based on the key and nonkey fields in the flow monitor's record and stored in the flow monitor cache.

**Examples**

The following example creates a flow monitor named FLOW-MONITOR-1 and enters flow monitor configuration mode:

```
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)#
```
flow record

To create a flow record, or to modify an existing flow record, and enter flow record configuration mode, use the `flow record` command in global configuration mode. To remove a record, use the `no` form of this command.

```
flow record record-name
no flow record record-name
```

### Syntax Description
- `record-name`: Name of the flow record that is being created or modified.

### Command Default
A flow record is not configured.

### Command Modes
Global configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines
A flow record defines the keys that use to identify packets in the flow, as well as other fields of interest that gathers for the flow. You can define a flow record with any combination of keys and fields of interest. The supports a rich set of keys. A flow record also defines the types of counters gathered per flow. You can configure 64-bit packet or byte counters.

### Examples
The following example creates a flow record named FLOW-RECORD-1, and enters flow record configuration mode:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)#
```
full-sector-dfs (mesh)

To configure mesh full sector Dynamic Frequency Selection (DFS) status for a mesh AP profile, use the `full-sector-dfs` command.

```plaintext
full-sector-dfs
```

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

Full sector DFS is enabled.

**Command Modes**

config-wireless-mesh-profile

**Command History**

<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>

**Example**

The following example shows how to configure mesh full sector DFS status for a mesh AP profile:

```plaintext
Device # configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device (config)# wireless profile mesh mesh-profile
Device (config-wireless-mesh-profile)# full-sector-dfs
```
Configuration Commands: g to z

- hyperlocation, on page 261
- idle-timeout, on page 262
- ids (mesh), on page 263
- inactive-timeout, on page 264
- interface vlan, on page 265
- ip access-group, on page 266
- ip access-list extended, on page 267
- ip address, on page 268
- ip admission, on page 271
- ip dhcp pool, on page 272
- ip dhcp-relay information option server-override, on page 273
- ip dhcp-relay source-interface, on page 275
- ip domain-name, on page 276
- ip flow monitor, on page 277
- ip flow-export destination, on page 278
- ip helper-address, on page 279
- ip http secure-server, on page 282
- ip http server, on page 284
- ip igmp snooping, on page 286
- ip multicast vlan, on page 287
- ip nbar protocol-discovery, on page 288
- ip nbar protocol-pack, on page 289
- ip ssh, on page 290
- ip ssh version, on page 291
- ip tftp blocksize, on page 293
- ip verify source, on page 294
- ipv4 dhcp, on page 295
- ipv4 flow monitor, on page 296
- ipv6 access-list, on page 297
- ipv6 address, on page 299
- ipv6 dhcp pool, on page 301
- ipv6 enable, on page 304
- ipv6 mld snooping, on page 306
• ipv6 nd managed-config-flag, on page 307
• ipv6 nd other-config-flag, on page 308
• ipv6 nd ra throttler attach-policy, on page 309
• ipv6 nd raguard policy, on page 310
• ipv6 snooping policy, on page 312
• ipv6 traffic-filter, on page 313
• key, on page 314
• ldap attribute-map, on page 315
• ldap server, on page 316
• local-auth ap eap-fast, on page 317
• local-site, on page 318
• location expiry, on page 319
• location notify-threshold, on page 320
• lsc-only-auth (mesh), on page 321
• mac-filtering, on page 322
• match (access-map configuration), on page 323
• match activated-service-template, on page 325
• match any, on page 327
• match application name, on page 328
• match interface, on page 330
• match ipv4, on page 331
• match ipv4, on page 332
• match ipv4 destination address, on page 333
• match ipv4 destination address, on page 334
• match ipv4 source address, on page 335
• match ipv4 source address, on page 336
• match ipv4 ttl, on page 337
• match ipv4 ttl, on page 338
• match ipv6, on page 339
• match ipv6, on page 340
• match ipv6 destination address, on page 341
• match ipv6 destination address, on page 342
• match ipv6 hop-limit, on page 343
• match ipv6 hop-limit, on page 344
• match ipv6 source address, on page 345
• match ipv6 source address, on page 346
• match message-type, on page 347
• match non-client-nrt, on page 348
• match protocol, on page 349
• match service-instance, on page 352
• match service-type, on page 353
• match transport, on page 354
• match transport, on page 355
• match transport icmp ipv4, on page 356
• match transport icmp ipv4, on page 357
• match transport icmp ipv6, on page 358
• match transport icmp ipv6, on page 359
• match user-role, on page 360
• match username, on page 361
• match wireless ssid (wireless), on page 362
• match wireless ssid (wireless), on page 363
• match (access-map configuration), on page 364
• match (class-map configuration), on page 366
• match wlan user-priority, on page 370
• max-bandwidth, on page 371
• max-through, on page 372
• method (mesh), on page 373
• method fast, on page 374
• mobility anchor, on page 375
• mop enabled, on page 377
• mop sysid, on page 378
• multicast, on page 379
• nac, on page 380
• nas-id option2, on page 381
• network, on page 382
• nmsp cloud-services enable, on page 383
• nmsp cloud-services http-proxy, on page 384
• nmsp cloud-services server token, on page 385
• nmsp cloud-services server url, on page 386
• nmsp notification interval, on page 387
• nmsp strong-cipher, on page 389
• office-extend, on page 390
• option, on page 391
• packet-capture, on page 393
• parameter-map type subscriber attribute-to-service, on page 394
• parameter-map type umbrella global, on page 395
• peer-blocking, on page 396
• policy, on page 397
• police, on page 398
• policy-tag, on page 400
• policy-map, on page 401
• policy-map, on page 403
• port, on page 405
• priority priority-value, on page 406
• priority-queue, on page 407
• priority, on page 409
• protocol (IPv6 snooping), on page 411
• qos queue-softmax-multiplier, on page 412
• qos video, on page 413
• qos wireless-default untrust, on page 414
• queue-buffers ratio, on page 415
• queue-limit, on page 416
• queue-set, on page 418
• radius server, on page 419
• range, on page 420
• reanchor class, on page 421
• record wireless avc basic, on page 422
• redundancy revertive, on page 423
• redirect , on page 424
• redirect portal , on page 425
• remote-span, on page 426
• remote-lan, on page 427
• request platform software trace archive, on page 428
• rf tag, on page 429
• rrc-evaluation, on page 430
• security , on page 431
• security dot1x authentication-list, on page 432
• security ft, on page 433
• security level (IPv6 snooping), on page 435
• security pmf, on page 436
• security static-wep-key , on page 438
• security web-auth, on page 439
• security wpa akm, on page 440
• service-policy (Wired), on page 442
• service-policy (WLAN), on page 444
• service-policy qos , on page 445
• service-template, on page 446
• session-timeout, on page 447
• set, on page 448
• set trace capwap ap ha, on page 455
• set trace mobility ha, on page 456
• set trace qos ap ha, on page 458
• sgt-tag, on page 459
• shutdown, on page 460
• site-tag, on page 461
• static-ip-mobility, on page 462
• switchport, on page 463
• switchport access vlan, on page 465
• switchport mode, on page 467
• tag rf, on page 469
• tag site, on page 470
• transport, on page 471
• trusted-port, on page 472
• type, on page 473
• udp-timeout, on page 474
• umbrella-param-map, on page 475
• username, on page 476
• violation, on page 478
• vlan, on page 479
• vlan configuration, on page 485
• vlan access-map, on page 486
• vlan filter, on page 488
• vlan group, on page 489
• wgbb broadcast-tagging, on page 490
• wgbb vlan, on page 491
• whitelist acl, on page 492
• config wlan assisted-roaming, on page 493
• wireless aaa policy, on page 494
• wireless aaa policy, on page 495
• wireless broadcast vlan, on page 496
• wireless client, on page 497
• wireless client mac-address, on page 500
• wireless config validate, on page 505
• wireless fabric control-plane, on page 507
• wireless fabric, on page 508
• wireless fabric name, on page 509
• wireless load-balancing, on page 510
• wireless macro-micro steering transition-threshold, on page 511
• wireless media-stream, on page 512
• wireless media-stream message, on page 514
• wireless media-stream multicast-direct, on page 515
• wireless mesh alarm association count, on page 516
• wireless mesh alarm high-snr, on page 517
• wireless mesh alarm low-snr, on page 518
• wireless mesh alarm max-children map, on page 519
• wireless mesh alarm max-children rap, on page 520
• wireless mesh alarm max-hop, on page 521
• wireless mesh alarm parent-change count, on page 522
• wireless mesh backhaul bdomain-channels, on page 523
• wireless mesh backhaul rrm, on page 524
• wireless mesh cac, on page 525
• wireless mesh ethernet-bridging allow-bdp, on page 526
• wireless mesh security psk provisioning, on page 527
• wireless mesh subset-channel-sync, on page 528
• wireless mobility, on page 529
• wireless mobility controller peer-group, on page 530
• wireless mobility group keepalive, on page 531
• wireless mobility group mac-address, on page 532
• wireless mobility group member ip, on page 533
• wireless mobility group multicast-address, on page 534
• wireless mobility group name, on page 535
• wireless mobility multicast ipv4, on page 536
• wireless mobility mac-address, on page 537
• wireless multicast, on page 538
• wireless profile airtime-fairness, on page 539
• wireless profile ap packet-capture, on page 540
• wireless profile fabric, on page 541
• wireless profile policy, on page 542
• wireless rfid, on page 543
• wireless security dot1x, on page 544
• wireless security dot1x radius accounting mac-delimiter, on page 546
• wireless security dot1x radius accounting username-delimiter, on page 547
• wireless security dot1x radius callStationIdCase, on page 548
• wireless security dot1x radius mac-authentication call-station-id, on page 549
• wireless security dot1x radius mac-authentication mac-delimiter, on page 550
• wireless security web-auth retries, on page 551
• wireless tag policy, on page 552
• wireless tag site, on page 553
• wireless wps ap-authentication, on page 554
• wireless wps client-exclusion, on page 555
• wireless wps rogue, on page 557
• wireless wps rogue ap rldp alarm-only, on page 558
• wireless wps rogue ap rldp auto-contain, on page 559
• wireless wps rogue client, on page 560
• wireless wps rogue detection, on page 561
• wireless wps rogue rule, on page 562
• wireless-default radius server, on page 564
• wlan policy, on page 565
hyperlocation

To configure Hyperlocation and related parameters for an AP group, use the `hyperlocation` command in the WLAN AP Group configuration (Device(config-apgroup)#) mode. To disable Hyperlocation and related parameter configuration for the AP group, use the `no` form of the command.

```
[no] hyperlocation [threshold {detection value-in-dBm | reset value-btwn-0-99 | trigger value-btwn-1-100}] }
```

Syntax Description

- `[no] hyperlocation` Enables or disables Hyperlocation for an AP group.
- `threshold detection value-in-dBm` Sets threshold to filter out packets with low RSSI. The `[no]` form of the command resets the threshold to its default value.
- `threshold reset value-btwn-0-99` Resets value in scan cycles after trigger. The `[no]` form of the command resets the threshold to its default value.
- `threshold trigger value-btwn-1-100` Sets the number of scan cycles before sending a BAR to clients. The `[no]` form of the command resets the threshold to its default value.

**Note** Ensure that the Hyperlocation threshold reset value is less than the threshold trigger value.

Command Modes

- WLAN AP Group configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Denali 16.3.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

- This example shows how to set threshold to filter out packets with low RSSI:
  ```
  Device(config-apgroup)# [no] hyperlocation threshold detection -100
  ```
- This example shows how to reset value in scan cycles after trigger:
  ```
  Device(config-apgroup)# [no] hyperlocation threshold reset 8
  ```
- This example shows how to set the number of scan cycles before sending a BAR to clients:
  ```
  Device(config-apgroup)# [no] hyperlocation threshold trigger 10
  ```
idle-timeout

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

```
idle-timeout value
```

**Syntax Description**

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

**Command Default**

None

**Command Modes**

config-wireless-policy

**Command History**

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

**Examples**

The following example shows how to set the idle-timeout in a wireless profile policy:

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

To configure IDS (Rogue/Signature Detection) reporting for outdoor mesh APs, use the `ids` command.

```
ids
```

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

IDS is disabled.

**Command Modes**

`config-wireless-mesh-profile`

**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>

**Example**

The following example shows how to configure IDS (Rogue/Signature Detection) reporting for outdoor mesh APs:

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

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

#### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>inactive-timeout</code></td>
<td><em>timeout-in-seconds</em></td>
</tr>
</tbody>
</table>

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

#### Command Default

None

#### Command Modes

ET-Analytics configuration

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

This example shows how to enable in-active timer in the ET-Analytics configuration mode:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# et-analytics
Device(config-et-analytics)# inactive-timeout 15
Device(config-et-analytics)# end
```
interface vlan

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

```
interface vlan vlan-id
no interface vlan vlan-id
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vlan-id</code></td>
<td>VLAN number. The range is 1 to 4094.</td>
</tr>
</tbody>
</table>

**Command Default**

The default VLAN interface is VLAN 1.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Note**

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

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

**Note**

You cannot delete the VLAN 1 interface.

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

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

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

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

```
Device(config)# interface vlan 23
Device(config-if)#
```
**ip access-group**

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

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

**Syntax Description**

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

**Command Default**

None

**Command Modes**

WLAN configuration

**Usage Guidelines**

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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

This example shows how to configure a WLAN ACL:

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

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

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

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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;100-199&gt;</td>
<td>Extended IP access-list number.</td>
</tr>
<tr>
<td>&lt;2000-2699&gt;</td>
<td>Extended IP access-list number (expanded range).</td>
</tr>
</tbody>
</table>

**Command Default:** None

**Command Modes:** Global configuration (config)

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure extended access list:

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

To set a primary or secondary IP address for an interface, use the `ip address` command in interface configuration mode. To remove an IP address or disable IP processing, use the `no` form of this command.

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

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip-address</code></td>
<td>IP address.</td>
</tr>
<tr>
<td><code>mask</code></td>
<td>Mask for the associated IP subnet.</td>
</tr>
<tr>
<td><code>secondary</code></td>
<td>(Optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address. If the secondary address is used for a VRF table configuration with the <code>vrf</code> keyword, the <code>vrf</code> keyword must be specified also.</td>
</tr>
<tr>
<td><code>vrf</code></td>
<td>(Optional) Name of the VRF table. The <code>vrf-name</code> argument specifies the VRF name of the ingress interface.</td>
</tr>
</tbody>
</table>

### Command Default

No IP address is defined for the interface.

### Command Modes

Interface configuration (config-if)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

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

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

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

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

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

- There may not be enough host addresses for a particular network segment. For example, your subnetting allows up to 254 hosts per logical subnet, but on one physical subnet you need 300 host addresses. Using
secondary IP addresses on the devices or access servers allows you to have two logical subnets using one physical subnet.

- Many older networks were built using Level 2 bridges. The judicious use of secondary addresses can aid in the transition to a subnetted, device-based network. Devices on an older, bridged segment can be easily made aware that many subnets are on that segment.

- Two subnets of a single network might otherwise be separated by another network. This situation is not permitted when subnets are in use. In these instances, the first network is extended, or layered on top of the second network using secondary addresses.

---

**Note**

If any device on a network segment uses a secondary address, all other devices on that same segment must also use a secondary address from the same network or subnet. Inconsistent use of secondary addresses on a network segment can very quickly cause routing loops.

---

**Note**

When you are routing using the Open Shortest Path First (OSPF) algorithm, ensure that all secondary addresses of an interface fall into the same OSPF area as the primary addresses.

To transparently bridge IP on an interface, you must perform the following two tasks:

- Disable IP routing (specify the `no ip routing` command).
- Add the interface to a bridge group, see the `bridge-group` command.

To concurrently route and transparently bridge IP on an interface, see the `bridge crb` command.

**Examples**

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

```
interface GigabitEthernet 1/0/1
ip address 192.108.1.27 255.255.255.0
ip address 192.31.7.17 255.255.255.0 secondary
```

**Related Commands**

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

To enable web authentication, use the **ip admission** command in interface configuration mode. You can also use this command in fallback-profile configuration mode. To disable web authentication, use the **no** form of this command.

```
ip admission  rule
no ip admission  rule
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rule</td>
<td>IP admission rule name.</td>
</tr>
</tbody>
</table>

**Command Default**

Web authentication is disabled.

**Command Modes**

Interface configuration

Fallback-profile configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The **ip admission** command applies a web authentication rule to a switch port.

This example shows how to apply a web authentication rule to a switchport:

```
Device# configure terminal
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip admission rule1
```

This example shows how to apply a web authentication rule to a fallback profile for use on an IEEE 802.1x enabled switch port.

```
Device# configure terminal
Device(config)# fallback profile profile1
Device(config-fallback-profile)# ip admission rule1
```
To configure a Dynamic Host Configuration Protocol (DHCP) address pool on a DHCP server and enter DHCP pool configuration mode, use the `ip dhcp pool` command in global configuration mode. To remove the address pool, use the `no` form of this command.

```
ip dhcp pool name
no ip dhcp pool name
```

**Syntax Description**

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

**Command Default**

DHCP address pools are not configured.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(1)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Examples**

The following example configures pool1 as the DHCP address pool:

```
ip dhcp pool pool1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>host</td>
<td>Specifies the IP address and network mask for a manual binding to a DHCP client.</td>
</tr>
<tr>
<td>ip dhcp excluded-address</td>
<td>Specifies IP addresses that a Cisco IOS DHCP server should not assign to DHCP clients.</td>
</tr>
<tr>
<td>network (DHCP)</td>
<td>Configures the subnet number and mask for a DHCP address pool on a Cisco IOS DHCP server.</td>
</tr>
</tbody>
</table>
ip dhcp-relay information option server-override

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

**Examples**

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

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip dhcp relay information option server-id-override</code></td>
<td>Enables the system to insert the server ID override and link selection suboptions on a specific interface into the DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server.</td>
</tr>
</tbody>
</table>
ip dhcp-relay source-interface

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

**ip dhcp-relay source-interface** *type* *number*

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

### Syntax Description

<table>
<thead>
<tr>
<th><strong>type</strong></th>
<th>Interface type. For more information, use the question mark (?) online help function.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>number</strong></td>
<td>Interface or subinterface number. For more information about the numbering system for your networking device, use the question mark (?) online help function.</td>
</tr>
</tbody>
</table>

### Command Default

The source interface is not configured.

### Command Modes

Global configuration (config)

### Command History

<table>
<thead>
<tr>
<th><strong>Release</strong></th>
<th>** Modification**</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was introduced on Cisco ASR 1000 Series Aggregation Services Routers.</td>
</tr>
<tr>
<td>12.2(33)SRE</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRE.</td>
</tr>
<tr>
<td>15.1(1)SY</td>
<td>This command was integrated into Cisco IOS Release 15.1(1)SY.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

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

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

### Examples

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

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

### Related Commands

<table>
<thead>
<tr>
<th><strong>Command</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>ip dhcp relay source-interface</td>
<td>Configures the source interface for the relay agent to use as the source IP address for relayed messages.</td>
</tr>
</tbody>
</table>
**ip domain-name**

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

```
ip domain-name domain-name [vrf vrf-name]
```

**Syntax Description**

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

**Command Default**

None

**Command Modes**

Global configuration (config)

**Command History**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure a host domain in a device:

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

To configure IP NetFlow monitoring, use the `ip flow monitor` command. To remove IP NetFlow monitoring, use the `no` form of this command.

```
ip flow monitor ip-monitor-name {input|output}
no ip flow monitor ip-monitor-name {input|output}
```

**Syntax Description**
- `ip-monitor-name` Flow monitor name.
- `input` Enables a flow monitor for ingress traffic.
- `output` Enables a flow monitor for egress traffic.

**Command Default**
None

**Command Modes**
WLAN configuration

**Usage Guidelines**
You must disable the WLAN before using this command.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE</td>
<td>This command was</td>
</tr>
<tr>
<td>3.2SE</td>
<td>introduced.</td>
</tr>
</tbody>
</table>

This example shows how to configure an IP flow monitor for the ingress traffic:

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

This example shows how to disable an IP flow monitor:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no ip flow monitor test input
```
ip flow-export destination

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

```
ip flow-export destination ip_address port_number
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Port_number</th>
<th>Port number. The range is from 1 to 65535.</th>
</tr>
</thead>
</table>

**Command Default**

None

**Command Modes**

ET-Analytics configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

This example shows how to configure ETA flow export destination in the ET-Analytics configuration mode:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# et-analytics
Device(config-et-analytics)# ip flow-export destination 120.0.0.1 2055
Device(config-et-analytics)# end
```
ip helper-address

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

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

**Syntax Description**

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

**Command Default**

UDP broadcasts are not forwarded.

**Command Modes**

Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(4)B</td>
<td>This command was modified. The <code>vrf name</code> keyword and argument pair and the <code>global</code> keyword were added.</td>
</tr>
<tr>
<td>12.2(15)T</td>
<td>This command was modified. The <code>redundancy vrg-name</code> keyword and argument pair was added.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

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

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

- The MAC address of the received frame must be all-ones broadcast address (ffff.ffff.ffff).
• The IP destination address must be one of the following: all-ones broadcast (255.255.255.255), subnet broadcast for the receiving interface, or major-net broadcast for the receiving interface if the no ip classless command is also configured.

• The IP time-to-live (TTL) value must be at least 2.

• The IP protocol must be UDP (17).

• The UDP destination port must be for TFTP, Domain Name System (DNS), Time, NetBIOS, ND, BOOTP or DHCP packet, or a UDP port specified by the ip forward-protocol udp command in global configuration mode.

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

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

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

Note

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

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

Examples

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

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

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

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

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

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip forward-protocol</code></td>
<td>Specifies which protocols and ports the router forwards when forwarding broadcast packets.</td>
</tr>
<tr>
<td><code>service dhcp</code></td>
<td>Enables the DHCP server and relay agent features on the router.</td>
</tr>
</tbody>
</table>
ip http secure-server

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

`ip http secure-server`  
`no ip http secure-server`

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

**Command Default**  
The HTTPS server is disabled.

**Command Modes**  
Global configuration (config)

**Command History**  

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

---

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

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

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

**Examples**

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

```
Device#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Device(config)#ip http secure-server  
Device(config)#ip http secure-trustpoint CA-trust-local  
Device(config)#end  
Device#show ip http server secure status  
HTTP secure server status: Enabled  
HTTP secure server port: 443  
HTTP secure server ciphersuite: 3des-ede-cbc-sha des-cbc-sha rc4-128-md5 rc4-12a  
HTTP secure server client authentication: Disabled  
HTTP secure server trustpoint: CA-trust-local
```
### Related Commands

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

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

```
ip http server
no ip http server
```

### Syntax Description

This command has no arguments or keywords.

### Command Default

The HTTP server uses the standard port 80 by default. HTTP/TCP port 8090 is open by default.

### Command Modes

Global configuration (config)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

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

⚠️ **Caution**

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

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

### Examples

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

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

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

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip http access-class</td>
<td>Specifies the access list that should be used to restrict access to the HTTP server.</td>
</tr>
<tr>
<td>ip http path</td>
<td>Specifies the base path used to locate files for use by the HTTP server.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>ip http secure-server</td>
<td>Enables the HTTPS server.</td>
</tr>
</tbody>
</table>
ip igmp snooping

To globally enable Internet Group Management Protocol (IGMP) snooping on the device or to enable it on a per-VLAN basis, use the `ip igmp snooping` global configuration command on the device stack or on a standalone device. To return to the default setting, use the `no` form of this command.

```
ip igmp snooping [vlan vlan-id]
no ip igmp snooping [vlan vlan-id]
```

**Syntax Description**

- `vlan vlan-id` (Optional) Enables IGMP snooping on the specified VLAN. Ranges are 1—1001 and 1006—4094.

**Command Default**

IGMP snooping is globally enabled on the device.

IGMP snooping is enabled on VLAN interfaces.

**Command Modes**

Global configuration

**Command History**

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

**Usage Guidelines**

When IGMP snooping is enabled globally, it is enabled in all of the existing VLAN interfaces. When IGMP snooping is globally disabled, it is disabled on all of the existing VLAN interfaces.

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs, and cannot be used in IGMP snooping.

**Example**

The following example shows how to globally enable IGMP snooping:

```
Device(config)# ip igmp snooping
```

The following example shows how to enable IGMP snooping on VLAN 1:

```
Device(config)# ip igmp snooping vlan 1
```

You can verify your settings by entering the `show ip igmp snooping` command in privileged EXEC mode.
To configure IP multicast on a single VLAN, use the `ip multicast vlan` command in global configuration mode. To remove the VLAN from the WLAN, use the `no` form of the command.

```
ip multicast vlan {vlan-name vlan-id}
no ip multicast vlan {vlan-name vlan-id}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-name</td>
<td>Specifies the VLAN name.</td>
</tr>
<tr>
<td>vlan-id</td>
<td>Specifies the VLAN ID.</td>
</tr>
</tbody>
</table>

**Command Default**

Disabled.

**Command Modes**

WLAN configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

None

This example configures vlan_id01 as a multicast VLAN.

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless multicast
Device(config)# wlan test-wlan 1
Device(config-wlan)# ip multicast vlan vlan_id01
```
ip nbar protocol-discovery

To configure application recognition on the wireless policy on enabling the NBAR2 engine, use the `ip nbar protocol-discovery` command.

**ip nbar protocol-discovery**

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>config-wireless-policy</td>
</tr>
<tr>
<td>Command History</td>
<td>Release</td>
</tr>
<tr>
<td></td>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure application recognition on the wireless policy:

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

To load the protocol pack from bootflash, use the `ip nbar protocol-pack` command.

```
ip nbar protocol-pack bootflash: [{force}]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>bootflash:</code></td>
<td>Load the protocol pack from bootflash:</td>
</tr>
<tr>
<td><code>force</code></td>
<td>Force load the Load protocol pack from the selected source.</td>
</tr>
</tbody>
</table>

### Command Default

None

### Command Modes

Global configuration (config)

### 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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to load the NBAR2 protocol pack from bootflash:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# ip nbar protocol-pack bootflash:
```
To configure Secure Shell (SSH) control parameters on your router, use the `ip ssh` command in global configuration mode. To restore the default value, use the `no` form of this command.

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

**Syntax Description**

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

**Command Default**

SSH control parameters are set to default router values.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.1(1)T</td>
<td>This command was integrated into Cisco IOS Release 12.1(1) T.</td>
</tr>
<tr>
<td>12.2(17a)SX</td>
<td>This command was integrated into Cisco IOS Release 12.2(17a)SX.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.4</td>
<td>This command was implemented on the Cisco ASR 1000 series routers.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Examples**

The following examples configure SSH control parameters on your router:

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

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

```
ip ssh version [{1|2}]
no ip ssh version [{1|2}]
```

**Syntax Description**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>(Optional) Router runs only SSH Version 1.</td>
</tr>
<tr>
<td>2</td>
<td>(Optional) Router runs only SSH Version 2.</td>
</tr>
</tbody>
</table>

**Command Default**

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

**Command Modes**

Global configuration

**Command History**

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

**Usage Guidelines**

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

**Examples**

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

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

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

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

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

```
Router (config)# no ip ssh version
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ip ssh</td>
<td>Displays debug messages for SSH.</td>
</tr>
<tr>
<td>disconnect ssh</td>
<td>Terminates a SSH connection on your router.</td>
</tr>
<tr>
<td>ip ssh</td>
<td>Configures SSH control parameters on your router.</td>
</tr>
<tr>
<td>ip ssh rsa keypair-name</td>
<td>Specifies which RSA key pair to use for a SSH connection.</td>
</tr>
<tr>
<td>show ip ssh</td>
<td>Displays the SSH connections of your router.</td>
</tr>
</tbody>
</table>
**ip tftp blocksize**

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

```
ip tftp blocksize blocksize-value
```

**Syntax Description**

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

**Command Default**

TFTP client blocksize is not configured.

**Command Modes**

- Global configuration (config)

**Command History**

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

**Usage Guidelines**

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

**Example**

The following example shows how to specify TFTP client blocksize:

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

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

```
ip verify source [mac-check] [tracking]
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac-check</td>
<td>(Optional) Enables IP source guard with MAC address verification.</td>
</tr>
<tr>
<td>tracking</td>
<td>(Optional) Enables IP port security to learn static IP address learning on a port.</td>
</tr>
</tbody>
</table>

**Command Default**

IP source guard is disabled.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

To enable IP source guard with source IP address filtering and MAC address verification, use the `ip verify source mac-check` interface configuration command.

**Examples**

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

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

This example shows how to enable IP source guard with MAC address verification:

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

You can verify your settings by entering the `show ip verify source` privileged EXEC command.
To configure the DHCP parameters for a WLAN, use the `ipv4 dhcp` command.

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

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

### Command Default
None

### Command Modes
- config-wireless-policy

### Command History
<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

### Examples
The following example shows how to configure DHCP address assignment as a requirement:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless profile policy demo-profile-name
Device(config-wireless-policy)# ipv4 dhcp required
```
To configure the IPv4 traffic ingress flow monitor for a WLAN profile policy, use the `ipv4 flow monitor input` command.

```
ipv4 flow monitor monitor-name input
```

**Syntax Description**

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

**Command Default**

None

**Command Modes**

config-wireless-policy

**Command History**

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

**Examples**

The following example shows how to configure the IPv4 traffic ingress flow monitor for a WLAN profile policy:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless profile policy policy-profile-name
Device(config-wireless-policy)# ipv4 flow monitor flow-monitor-name input
```
**ipv6 access-list**

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

```
ipv6 access-list access-list-name | match-local-traffic | log-update threshold threshold-in-msgs |
role-based list-name
no ipv6 access-list access-list-name |
client permit-control-packets | log-update threshold | role-based list-name
```

### Syntax Description

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

### Command Default

No IPv6 access list is defined.

### Command Modes

Global configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Denali 16.3.1</td>
<td>This command was reintroduced. This command was not supported in Cisco IOS XE Denali 16.1.x and Cisco IOS XE Denali 16.2.x</td>
</tr>
</tbody>
</table>

### Usage Guidelines

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

Note

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

IPv6 is automatically configured as the protocol type in `permit any any` and `deny any any` statements that are translated from global configuration mode to IPv6 access list configuration mode.
Every IPv6 ACL has implicit **permit icmp any any nd-na**, **permit icmp any any nd-ns**, and **deny ipv6 any any** statements as its last match conditions. (The former two match conditions allow for ICMPv6 neighbor discovery.) An IPv6 ACL must contain at least one entry for the implicit **deny ipv6 any any** statement to take effect. The IPv6 neighbor discovery process makes use of the IPv6 network layer service; therefore, by default, IPv6 ACLs implicitly allow IPv6 neighbor discovery packets to be sent and received on an interface. In IPv4, the Address Resolution Protocol (ARP), which is equivalent to the IPv6 neighbor discovery process, makes use of a separate data link layer protocol; therefore, by default, IPv4 ACLs implicitly allow ARP packets to be sent and received on an interface.

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

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

**Examples**

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

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

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

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

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

```
ipv6 address {ipv6-prefix/prefix-length|prefix-name sub-bits/prefix-length}

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

**Syntax Description**

<table>
<thead>
<tr>
<th><code>ipv6-address</code></th>
<th>The IPv6 address to be used.</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>/ prefix-length</code></td>
<td>The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.</td>
</tr>
<tr>
<td><code>prefix-name</code></td>
<td>A general prefix, which specifies the leading bits of the network to be configured on the interface.</td>
</tr>
<tr>
<td><code>sub-bits</code></td>
<td>The subprefix bits and host bits of the address to be concatenated with the prefixes provided by the general prefix specified with the <code>prefix-name</code> argument. The <code>sub-bits</code> argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.</td>
</tr>
</tbody>
</table>

**Command Default**

No IPv6 addresses are defined for any interface.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(2)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(25)SG</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)SG.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was integrated into Cisco ASR 1000 Series devices.</td>
</tr>
<tr>
<td>15.2(4)S</td>
<td>This command was integrated into Cisco IOS Release 15.2(4)S.</td>
</tr>
<tr>
<td>15.2(2)SNG</td>
<td>This command was implemented on the Cisco ASR 901 Series Aggregation Services devices.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.2SE</td>
<td>This command was integrated into Cisco IOS XE Release 3.2SE.</td>
</tr>
</tbody>
</table>
The `ipv6 address` command allows multiple IPv6 addresses to be configured on an interface in various different ways, with varying options. The most common way is to specify the IPv6 address with the prefix length.

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

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

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

### Examples

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

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

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

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6 address anycast</code></td>
<td>Configures an IPv6 anycast address and enables IPv6 processing on an interface.</td>
</tr>
<tr>
<td><code>ipv6 address eui-64</code></td>
<td>Configures an IPv6 address and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address.</td>
</tr>
<tr>
<td><code>ipv6 address link-local</code></td>
<td>Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface.</td>
</tr>
<tr>
<td><code>ipv6 unnumbered</code></td>
<td>Enables IPv6 processing on an interface without assigning an explicit IPv6 address to the interface.</td>
</tr>
<tr>
<td><code>no ipv6 address autoconfig</code></td>
<td>Removes all IPv6 addresses from an interface.</td>
</tr>
<tr>
<td><code>show ipv6 interface</code></td>
<td>Displays the usability status of interfaces configured for IPv6.</td>
</tr>
</tbody>
</table>
**ipv6 dhcp pool**

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

```
ipv6 dhcp pool poolname
no ipv6 dhcp pool poolname
```

**Syntax Description**

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

**Command Default**

DHCP for IPv6 pools are not configured.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(4)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(18)SXE</td>
<td>This command was integrated into Cisco IOS Release 12.2(18)SXE.</td>
</tr>
<tr>
<td>12.4(24)T</td>
<td>This command was integrated into Cisco IOS Release 12.4(24)T.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was integrated into Cisco IOS XE Release 2.1.</td>
</tr>
<tr>
<td>12.2(33)SRE</td>
<td>This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.</td>
</tr>
<tr>
<td>12.2(33)XNE</td>
<td>This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

- **address prefix IPv6-prefix [lifetime [valid-lifetime preferred-lifetime | infinite]]** sets an address prefix for address assignment. This address must be in hexadecimal, using 16-bit values between colons.
- **link-address IPv6-prefix** sets a link-address IPv6 prefix. When an address on the incoming interface or a link-address in the packet matches the specified IPv6-prefix, the server uses the configuration information pool. This address must be in hexadecimal, using 16-bit values between colons.
- **vendor-specific vendor-id** enables DHCPv6 vendor-specific configuration mode. Specify a vendor identification number. This number is the vendor IANA Private Enterprise Number. The range is 1 to 4294967295. The following configuration command is available:
  - **suboption number** sets vendor-specific suboption number. The range is 1 to 65535. You can enter an IPv6 address, ASCII text, or a hex string as defined by the suboption parameters.
The hex value used under the suboption keyword allows users to enter only hex digits (0-f). Entering an invalid hex value does not delete the previous configuration.

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

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

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

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

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

**Examples**

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

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

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

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

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

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

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

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 dhcp server</td>
<td>Enables DHCP for IPv6 service on an interface.</td>
</tr>
<tr>
<td>show ipv6 dhcp pool</td>
<td>Displays DHCP for IPv6 configuration pool information.</td>
</tr>
</tbody>
</table>
ipv6 enable

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

```
ipv6 enable
no ipv6 enable
```

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

**Command Default**
IPv6 is disabled.

**Command Modes**
Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(2)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(21)ST</td>
<td>This command was integrated into Cisco IOS Release 12.0(21)ST.</td>
</tr>
<tr>
<td>12.0(22)S</td>
<td>This command was integrated into Cisco IOS Release 12.0(22)S.</td>
</tr>
<tr>
<td>12.2(14)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(14)S.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(25)SG</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)SG.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was integrated into Cisco IOS XE Release 2.1.</td>
</tr>
<tr>
<td>15.2(2)SNG</td>
<td>This command was implemented on the Cisco ASR 901 Series Aggregation Services devices.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.2SE</td>
<td>This command was integrated into Cisco IOS XE Release 3.2SE.</td>
</tr>
<tr>
<td>15.2(2)SA2</td>
<td>This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.</td>
</tr>
</tbody>
</table>

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

**Examples**
The following example enables IPv6 processing on Ethernet interface 0/0:
Device(config)# interface ethernet 0/0
Device(config-if)# ipv6 enable

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 address link-local</td>
<td>Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface.</td>
</tr>
<tr>
<td>ipv6 address eui-64</td>
<td>Configures an IPv6 address and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address.</td>
</tr>
<tr>
<td>ipv6 unnumbered</td>
<td>Enables IPv6 processing on an interface without assigning an explicit IPv6 address to the interface.</td>
</tr>
<tr>
<td>show ipv6 interface</td>
<td>Displays the usability status of interfaces configured for IPv6.</td>
</tr>
</tbody>
</table>
ipv6 mld snooping

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

```
ipv6 mld snooping
no ipv6 mld snooping
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

This command is enabled.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(18)SXE</td>
<td>This command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>15.4(2)S</td>
<td>This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

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

**Examples**

This example shows how to enable MLDv2 snooping globally:

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipv6 mld snooping</td>
<td>Displays MLDv2 snooping information.</td>
</tr>
</tbody>
</table>
ipv6 nd managed-config-flag

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

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

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

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

**Command Modes**

Interface configuration

**Command History**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

Hosts may use stateful and stateless address autoconfiguration simultaneously.

**Examples**

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

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

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

```
ipv6 nd other-config-flag
```

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

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

**Command Modes**

- Interface configuration
- Dynamic template configuration

**Command History**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Note**

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

**Examples**

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

```
Device(config)# interface
Device(config-if)# ipv6 nd other-config-flag
```
ipv6 nd ra throttler attach-policy

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

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

**Syntax Description**

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

**Command Default**

None

**Command Modes**

- `config-vlan`

**Command History**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure configure a IPv6 policy for feature RA throttler:

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

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

```
ipv6 nd raguard policy policy-name
```

**Syntax Description**

- `policy-name` IPv6 RA guard policy name.

**Command Default**

An RA guard policy is not configured.

**Command Modes**

Global configuration (config)"

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(50)SY</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.2(4)S</td>
<td>This command was integrated into Cisco IOS Release 15.2(4)S.</td>
</tr>
<tr>
<td>15.0(2)SE</td>
<td>This command was integrated into Cisco IOS Release 15.0(2)SE.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.2SE</td>
<td>This command was integrated into Cisco IOS XE Release 3.2SE.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

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

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

**Examples**

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

```
Device(config)# ipv6 nd raguard policy policy1
Device(config-ra-guard)#
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>device-role</td>
<td>Specifies the role of the device attached to the port.</td>
</tr>
<tr>
<td>drop-unsecure</td>
<td>Drops messages with no or invalid options or an invalid signature.</td>
</tr>
<tr>
<td>ipv6 nd raguard attach-policy</td>
<td>Applies the IPv6 RA guard feature on a specified interface.</td>
</tr>
<tr>
<td>limit address-count</td>
<td>Limits the number of IPv6 addresses allowed to be used on the port.</td>
</tr>
<tr>
<td>sec-level minimum</td>
<td>Specifies the minimum security level parameter value when CGA options are used.</td>
</tr>
<tr>
<td>trusted-port</td>
<td>Configures a port to become a trusted port.</td>
</tr>
<tr>
<td>validate source-mac</td>
<td>Checks the source MAC address against the link layer address.</td>
</tr>
</tbody>
</table>
**ipv6 snooping policy**

*Note*  
All existing IPv6 Snooping commands (prior to Cisco IOS XE Denali 16.1.1) now have corresponding SISF-based device-tracking commands that allow you to apply your configuration to both IPv4 and IPv6 address families. For more information, see [device-tracking policy](#).

To configure an IPv6 snooping policy and enter IPv6 snooping configuration mode, use the `ipv6 snooping policy` command in global configuration mode. To delete an IPv6 snooping policy, use the `no` form of this command.

```
ipv6 snooping policy  snooping-policy
no ipv6 snooping policy  snooping-policy
```

**Syntax Description**

- `snooping-policy`  
  User-defined name of the snooping policy. The policy name can be a symbolic string (such as Engineering) or an integer (such as 0).

**Command Default**

An IPv6 snooping policy is not configured.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `ipv6 snooping policy` command to create an IPv6 snooping policy. When the `ipv6 snooping policy` command is enabled, the configuration mode changes to IPv6 snooping configuration mode. In this mode, the administrator can configure the following IPv6 first-hop security commands:

- The `device-role` command specifies the role of the device attached to the port.
- The `limit address-count maximum` command limits the number of IPv6 addresses allowed to be used on the port.
- The `protocol` command specifies that addresses should be gleaned with Dynamic Host Configuration Protocol (DHCP) or Neighbor Discovery Protocol (NDP).
- The `security-level` command specifies the level of security enforced.
- The `tracking` command overrides the default tracking policy on a port.
- The `trusted-port` command configures a port to become a trusted port; that is, limited or no verification is performed when messages are received.

This example shows how to configure an IPv6 snooping policy:

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)#
```


**ipv6 traffic-filter**

This command enables IPv6 traffic filter.

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

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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>web</th>
<th>(Optional) Specifies an IPv6 access name for the WLAN Web ACL.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>acl-name</td>
<td>Specifies an IPv6 access name.</td>
</tr>
</tbody>
</table>

**Command Default**

Filtering of IPv6 traffic on an interface is not configured.

**Command Modes**

wlan

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

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

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

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

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

```
Device(config-wlan)# ipv6 traffic-filter TestDocTrafficFilter
```
To identify an authentication key on a key chain, use the `key` command in key-chain configuration mode. To remove the key from the key chain, use the `no` form of this command.

```
key key-id
no key key-id
```

**Syntax Description**

| `key-id` | Identification number of an authentication key on a key chain. The range of keys is from 0 to 2147483647. The key identification numbers need not be consecutive. |

**Command Default**

No key exists on the key chain.

**Command Modes**

Key-chain configuration (config-keychain)

**Usage Guidelines**

It is useful to have multiple keys on a key chain so that the software can sequence through the keys as they become invalid after time, based on the `accept-lifetime` and `send-lifetime` key chain key command settings.

Each key has its own key identifier, which is stored locally. The combination of the key identifier and the interface associated with the message uniquely identifies the authentication algorithm and Message Digest 5 (MD5) authentication key in use. Only one authentication packet is sent, regardless of the number of valid keys. The software starts looking at the lowest key identifier number and uses the first valid key.

If the last key expires, authentication will continue and an error message will be generated. To disable authentication, you must manually delete the last valid key.

To remove all keys, remove the key chain by using the `no key chain` command.

**Examples**

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

```
Device(config-keychain)# key 1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>accept-lifetime</code></td>
<td>Sets the time period during which the authentication key on a key chain is received as valid.</td>
</tr>
<tr>
<td><code>key chain</code></td>
<td>Defines an authentication key chain needed to enable authentication for routing protocols.</td>
</tr>
<tr>
<td><code>key-string (authentication)</code></td>
<td>Specifies the authentication string for a key.</td>
</tr>
<tr>
<td><code>send-lifetime</code></td>
<td>Sets the time period during which an authentication key on a key chain is valid to be sent.</td>
</tr>
<tr>
<td><code>show key chain</code></td>
<td>Displays authentication key information.</td>
</tr>
</tbody>
</table>
## ldap attribute-map

To configure a dynamic attribute map on an SLDAP server, use the `ldap attribute-map` command.

```
ldap attribute-map  map-name
```

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>Global configuration (config)</td>
</tr>
<tr>
<td>Command History</td>
<td><strong>Release</strong></td>
</tr>
<tr>
<td></td>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
</tr>
</tbody>
</table>

This example shows how to configure a dynamic attribute map on an SLDAP server:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ldap attribute-map map1
Device(config-attr-map)# map type department supplicant-group
Device(config-attr-map)# exit
```
To configure secure LDAP, use the `ldap server` command.

```
ldap server name
```

**Syntax Description**

<table>
<thead>
<tr>
<th>name</th>
<th>Server name.</th>
</tr>
</thead>
</table>

**Command Default**

None

**Command Modes**

Global configuration (config)

**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>

**Example**

This example shows how to configure secure LDAP:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# ldap server server1
Device(config-ldap-server)# ipv4 9.4.109.20
Device(config-ldap-server)# timeout retransmit 20
Device(config-ldap-server)# bind authenticate root-dn CN=ldapipv6user,CN=Users,DC=ca,DC=ssh2,DC=com password Cisco12345
Device(config-ldap-server)# base-dn CN=Users,DC=ca,DC=ssh2,DC=com
Device(config-ldap-server)# mode secure no- negotiation
Device(config-ldap-server)# end
```
**local-auth ap eap-fast**

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

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

**Syntax Description**

<table>
<thead>
<tr>
<th>profile-name</th>
<th>Enter eap-fast profile name.</th>
</tr>
</thead>
</table>

**Command Default**

None

**Command Modes**

config-wireless-flex-profile

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure EAP Fast method authentication on a Flex policy:

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

```
local-site
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>local-site</code></td>
<td>Configure this site as local site.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

config-site-tag

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to set the current site as local site:

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

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

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

Syntax Description

<table>
<thead>
<tr>
<th>calibrating-client</th>
<th>Timeout value for calibrating clients.</th>
</tr>
</thead>
<tbody>
<tr>
<td>client</td>
<td>Timeout value for clients.</td>
</tr>
<tr>
<td>tags</td>
<td>Timeout value for RFID tags.</td>
</tr>
<tr>
<td>timeout-duration</td>
<td>Timeout duration, in seconds.</td>
</tr>
</tbody>
</table>

Command Default

Timeout value is not configured.

Command Modes

Global configuration (config)

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>

Example

This example shows how to configure the location expiry duration:

Device(config)# location expiry tags 50
To configure the NMSP notification threshold for RSSI measurements, use the `location notify-threshold` command in global configuration mode. To remove the NMSP notification threshold for RSSI measurements, use the `no` form of this command.

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

### Syntax Description

- **client**: Specifies the NMSP notification threshold (in dB) for clients and rogue clients.
  - The valid range for the threshold parameter is 0 to 10 dB, and the default value is 0 dB.

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

- **tags**: Specifies the NMSP notification threshold (in dB) for RFID tags.
  - The valid range for the threshold parameter is 0 to 10 dB, and the default value is 0 dB.

- **db**: The valid range for the threshold parameter is 0 to 10 dB, and the default value is 0 dB.

### Command Default

No default behavior or values.

### Command Modes

Global configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

```
Device# configure terminal
Device(config)# location notify-threshold client 10
Device(config)# end
```
To configure mesh security to Locally Significant Certificate (LSC) only MAP authentication, use the `lsc-only-auth` command.

### Syntax Description

This command has no keywords or arguments.

### Command Default

LSC only authentication is enabled.

### Command Modes

`config-wireless-mesh-profile`

### 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>

### Example

The following example shows how to configure mesh security to LSC only MAP authentication:

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

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

```
mac-filtering [mac-authorization-list]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Name of the Authorization list.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Command Modes</th>
<th>config-wlan</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Modification</td>
</tr>
<tr>
<td></td>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
</tr>
<tr>
<td></td>
<td>This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enable MAC filtering on a WLAN:

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

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

```
match {ip address {namenumber} [{namenumber}] [{namenumber}]...|ipv6 address {namenumber} [{namenumber}] [{namenumber}]...|mac address {name} [{name}] [{name}]...}
```

```
no match {ip address {namenumber} [{namenumber}] [{namenumber}]...|ipv6 address {namenumber} [{namenumber}] [{namenumber}]...|mac address {name} [{name}] [{name}]...}
```

**Syntax Description**

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

**Command Default**

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

**Command Modes**

Access-map configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

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

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

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

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

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

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

You can verify your settings by entering the `show vlan access-map` privileged EXEC command.
match activated-service-template

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

```
match activated-service-template template-name
no-match activated-service-template template-name
```

**Syntax Description**

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

**Command Default**

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

**Command Modes**

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

**Command History**

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

**Usage Guidelines**

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

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

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

**Examples**

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

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>activate (policy-map action)</code></td>
<td>Activates a control policy or service template on a subscriber session.</td>
</tr>
<tr>
<td><code>class</code></td>
<td>Associates a control class with one or more actions in a control policy.</td>
</tr>
<tr>
<td><code>match service-template</code></td>
<td>Creates a condition that evaluates true based on an event’s service template.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>service-template</td>
<td>Defines a template that contains a set of service policy attributes to apply to subscriber sessions.</td>
</tr>
</tbody>
</table>
match any

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

```plaintext
match any
```

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>config-cmap</td>
</tr>
</tbody>
</table>

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to match any packet passing through the device:

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

To configure the use of the application name as a key field for a flow record, use the **match application name** command in flow record configuration mode. To disable the use of the application name as a key field for a flow record, use the **no** form of this command.

**match application name**

**no match application name**

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

The application name is not configured as a key field.

**Command Modes**

Flow record configuration (config-flow-record)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.2(2)T</td>
<td>This command was integrated into Cisco IOS Release 15.2(2)T for Cisco</td>
</tr>
<tr>
<td></td>
<td>Performance Monitor.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.5S</td>
<td>This command was integrated into Cisco IOS XE Release 3.5S for Cisco</td>
</tr>
<tr>
<td></td>
<td>Performance Monitor.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command, however the mode prompt is the same for both products. For Performance Monitor, you must first enter the **flow record type performance-monitor** command before you can use this command.

Because the mode prompt is the same for both products, here we refer to the command mode for both products as flow record configuration mode. However, for Flexible NetFlow, the mode is also known as Flexible NetFlow flow record configuration mode; and for Performance Monitor, the mode is also known as Performance Monitor flow record configuration mode.

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

**Examples**

The following example configures the application name as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match application name
```

**Cisco Performance Monitor in Cisco IOS Release 15.2(2)T and XE 3.5S**

The following example configures the application name as a key field:
Router(config)# flow record type performance-monitor RECORD-1
Router(config-flow-record)# match application name

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>collect application name</td>
<td>Configures the use of application name as a nonkey field for a Flexible NetFlow flow record.</td>
</tr>
<tr>
<td></td>
<td>flow record</td>
<td>Creates a flow record, and enters Flexible NetFlow flow record configuration mode.</td>
</tr>
<tr>
<td></td>
<td>flow record type performance-monitor</td>
<td>Creates a flow record, and enters Performance Monitor flow record configuration mode.</td>
</tr>
</tbody>
</table>
**match interface**

To configure the input and output interfaces as key fields for a flow record, use the `match interface` command in flow record configuration mode. To disable the use of the input and output interfaces as key fields for a flow record, use the `no` form of this command.

```
match interface {input|output}
```

```
no match interface {input|output}
```

**Syntax Description**

- **input**: Configures the input interface as a key field.
- **output**: Configures the output interface as a key field.

**Command Default**

The input and output interfaces are not configured as key fields.

**Command Modes**

Flow record configuration

**Command History**

```
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
```

**Usage Guidelines**

A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the `match` command.

The following example configures the input interface as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match interface input
```

The following example configures the output interface as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match interface output
```
**match ipv4**

To configure one or more of the IPv4 fields as a key field for a flow record, use the `match ipv4` command in flow record configuration mode. To disable the use of one or more of the IPv4 fields as a key field for a flow record, use the `no` form of this command.

```
match ipv4 {destination address|protocol|source address|tos|version}
no match ipv4 {destination address|protocol|source address|tos|version}
```

**Syntax Description**

- **destination address**: Configures the IPv4 destination address as a key field. For more information see `match ipv4 destination address`, on page 333.
- **protocol**: Configures the IPv4 protocol as a key field.
- **source address**: Configures the IPv4 destination address as a key field. For more information see `match ipv4 source address`, on page 335.
- **tos**: Configures the IPv4 ToS as a key field.
- **version**: Configures the IP version from IPv4 header as a key field.

**Command Default**

The use of one or more of the IPv4 fields as a key field for a user-defined flow record is not enabled.

**Command Modes**

Flow record configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the `match` command.

The following example configures the IPv4 protocol as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv4 protocol
```
**match ipv4**

To configure one or more of the IPv4 fields as a key field for a flow record, use the `match ipv4` command in flow record configuration mode. To disable the use of one or more of the IPv4 fields as a key field for a flow record, use the `no` form of this command.

```plaintext
match ipv4 {destination address|protocol|source address|tos|version}
no match ipv4 {destination address|protocol|source address|tos|version}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>destination address</code></td>
<td>Configures the IPv4 destination address as a key field. For more information see <code>match ipv4 destination address</code>, on page 333.</td>
</tr>
<tr>
<td><code>protocol</code></td>
<td>Configures the IPv4 protocol as a key field.</td>
</tr>
<tr>
<td><code>source address</code></td>
<td>Configures the IPv4 destination address as a key field. For more information see <code>match ipv4 source address</code>, on page 335.</td>
</tr>
<tr>
<td><code>tos</code></td>
<td>Configures the IPv4 ToS as a key field.</td>
</tr>
<tr>
<td><code>version</code></td>
<td>Configures the IP version from IPv4 header as a key field.</td>
</tr>
</tbody>
</table>

### Command Default
The use of one or more of the IPv4 fields as a key field for a user-defined flow record is not enabled.

### Command Modes
Flow record configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the `match` command.

The following example configures the IPv4 protocol as a key field:

```plaintext
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv4 protocol
```
match ipv4 destination address

To configure the IPv4 destination address as a key field for a flow record, use the **match ipv4 destination address** command in flow record configuration mode. To disable the IPv4 destination address as a key field for a flow record, use the **no** form of this command.

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

The IPv4 destination address is not configured as a key field.

**Command Modes**

Flow record configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

To return this command to its default settings, use the **no match ipv4 destination address** or **default match ipv4 destination address** flow record configuration command.

The following example configures the IPv4 destination address as a key field for a flow record:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv4 destination address
```
match ipv4 destination address

To configure the IPv4 destination address as a key field for a flow record, use the **match ipv4 destination address** command in flow record configuration mode. To disable the IPv4 destination address as a key field for a flow record, use the **no** form of this command.

**match ipv4 destination address**

**no match ipv4 destination address**

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

### Command Default
The IPv4 destination address is not configured as a key field.

### Command Modes
Flow record configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines
A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

To return this command to its default settings, use the **no match ipv4 destination address** or **default match ipv4 destination address** flow record configuration command.

The following example configures the IPv4 destination address as a key field for a flow record:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv4 destination address
```
match ipv4 source address

To configure the IPv4 source address as a key field for a flow record, use the `match ipv4 source address` command in flow record configuration mode. To disable the use of the IPv4 source address as a key field for a flow record, use the `no` form of this command.

```
match ipv4 source address
no match ipv4 source address
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

The IPv4 source address is not configured as a key field.

**Command Modes**

Flow record configuration

**Command History**

```
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
```

**Usage Guidelines**

A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the `match` command.

To return this command to its default settings, use the `no match ipv4 source address` or `default match ipv4 source address` flow record configuration command.

The following example configures the IPv4 source address as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv4 source address
```
match ipv4 source address

To configure the IPv4 source address as a key field for a flow record, use the `match ipv4 source address` command in flow record configuration mode. To disable the use of the IPv4 source address as a key field for a flow record, use the `no` form of this command.

```plaintext
match ipv4 source address
no match ipv4 source address
```

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

**Command Default**
The IPv4 source address is not configured as a key field.

**Command Modes**
Flow record configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the `match` command.

To return this command to its default settings, use the `no match ipv4 source address` or `default match ipv4 source address` flow record configuration command.

The following example configures the IPv4 source address as a key field:

```plaintext
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv4 source address
```
**match ipv4 ttl**

To configure the IPv4 time-to-live (TTL) field as a key field for a flow record, use the `match ipv4 ttl` command in flow record configuration mode. To disable the use of the IPv4 TTL field as a key field for a flow record, use the `no` form of this command.

``` untersuchung match ipv4 ttl
no match ipv4 ttl
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

The IPv4 time-to-live (TTL) field is not configured as a key field.

**Command Modes**

Flow record configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the `match ipv4 ttl` command.

The following example configures IPv4 TTL as a key field:

``` untersuchung
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv4 ttl
```
**match ipv4 ttl**

To configure the IPv4 time-to-live (TTL) field as a key field for a flow record, use the `match ipv4 ttl` command in flow record configuration mode. To disable the use of the IPv4 TTL field as a key field for a flow record, use the `no` form of this command.

```
match ipv4 ttl
no match ipv4 ttl
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>This command has no arguments or keywords.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Default</td>
<td>The IPv4 time-to-live (TTL) field is not configured as a key field.</td>
</tr>
<tr>
<td>Command Modes</td>
<td>Flow record configuration</td>
</tr>
<tr>
<td>Command History</td>
<td><strong>Release</strong></td>
</tr>
<tr>
<td></td>
<td>Cisco IOS XE 3.2SE</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the `match ipv4 ttl` command.

The following example configures IPv4 TTL as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv4 ttl
```
match ipv6

To configure one or more of the IPv6 fields as a key field for a flow record, use the **match ipv6** command in flow record configuration mode. To disable the use of one or more of the IPv6 fields as a key field for a flow record, use the **no** form of this command.

**Syntax**

```
match ipv6 {destination address|protocol|source address|traffic-class|version}
no match ipv6 {destination address|protocol|source address|traffic-class|version}
```

**Syntax Description**

- **destination address**: Configures the IPv4 destination address as a key field. For more information see `match ipv6 destination address, on page 341.`
- **protocol**: Configures the IPv6 protocol as a key field.
- **source address**: Configures the IPv4 destination address as a key field. For more information see `match ipv6 source address, on page 345.`

**Command Default**

The IPv6 fields are not configured as a key field.

**Command Modes**

Flow record configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

The following example configures the IPv6 protocol field as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv6 protocol
```
match ipv6

To configure one or more of the IPv6 fields as a key field for a flow record, use the **match ipv6** command in flow record configuration mode. To disable the use of one or more of the IPv6 fields as a key field for a flow record, use the **no** form of this command.

```
match ipv6 {destination address|protocol|source address|traffic-class|version}
no match ipv6 {destination address|protocol|source address|traffic-class|version}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>destination address</td>
<td>Configures the IPv4 destination address as a key field. For more information see match ipv6 destination address, on page 341.</td>
</tr>
<tr>
<td>protocol</td>
<td>Configures the IPv6 protocol as a key field.</td>
</tr>
<tr>
<td>source address</td>
<td>Configures the IPv4 destination address as a key field. For more information see match ipv6 source address, on page 345.</td>
</tr>
</tbody>
</table>

### Command Default

The IPv6 fields are not configured as a key field.

### Command Modes

Flow record configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

The following example configures the IPv6 protocol field as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv6 protocol
```
**match ipv6 destination address**

To configure the IPv6 destination address as a key field for a flow record, use the `match ipv6 destination address` command in flow record configuration mode. To disable the IPv6 destination address as a key field for a flow record, use the `no form of this command.

```
match ipv6 destination address
no match ipv6 destination address
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

The IPv6 destination address is not configured as a key field.

**Command Modes**

Flow record configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the `match` command.

To return this command to its default settings, use the `no match ipv6 destination address` or `default match ipv6 destination address` flow record configuration command.

The following example configures the IPv6 destination address as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv6 destination address
```
match ipv6 destination address

To configure the IPv6 destination address as a key field for a flow record, use the `match ipv6 destination address` command in flow record configuration mode. To disable the IPv6 destination address as a key field for a flow record, use the `no` form of this command.

```
match ipv6 destination address
no match ipv6 destination address
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

The IPv6 destination address is not configured as a key field.

**Command Modes**

Flow record configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the `match` command.

To return this command to its default settings, use the `no match ipv6 destination address` or `default match ipv6 destination address` flow record configuration command.

The following example configures the IPv6 destination address as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv6 destination address
```
**match ipv6 hop-limit**

To configure the IPv6 hop limit as a key field for a flow record, use the `match ipv6 hop-limit` command in flow record configuration mode. To disable the use of a section of an IPv6 packet as a key field for a flow record, use the `no` form of this command.

```
match ipv6 hop-limit
no match ipv6 hop-limit
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

The use of the IPv6 hop limit as a key field for a user-defined flow record is not enabled by default.

**Command Modes**

Flow record configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the `match` command.

The following example configures the hop limit of the packets in the flow as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv6 hop-limit
```
**match ipv6 hop-limit**

To configure the IPv6 hop limit as a key field for a flow record, use the `match ipv6 hop-limit` command in flow record configuration mode. To disable the use of a section of an IPv6 packet as a key field for a flow record, use the `no` form of this command.

```
match ipv6 hop-limit
no match ipv6 hop-limit
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

The use of the IPv6 hop limit as a key field for a user-defined flow record is not enabled by default.

**Command Modes**

Flow record configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the `match` command.

The following example configures the hop limit of the packets in the flow as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv6 hop-limit
```
**match ipv6 source address**

To configure the IPv6 source address as a key field for a flow record, use the `match ipv6 source address` command in flow record configuration mode. To disable the use of the IPv6 source address as a key field for a flow record, use the `no` form of this command.

```
match ipv6 source address
no match ipv6 source address
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

The IPv6 source address is not configured as a key field.

**Command Modes**

Flow record configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the `match` command.

To return this command to its default settings, use the `no match ipv6 source address` or `default match ipv6 source address` flow record configuration command.

The following example configures a IPv6 source address as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv6 source address
```
**match ipv6 source address**

To configure the IPv6 source address as a key field for a flow record, use the `match ipv6 source address` command in flow record configuration mode. To disable the use of the IPv6 source address as a key field for a flow record, use the `no` form of this command.

```
match ipv6 source address
no match ipv6 source address
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

The IPv6 source address is not configured as a key field.

**Command Modes**

Flow record configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the `match` command.

To return this command to its default settings, use the `no match ipv6 source address` or `default match ipv6 source address` flow record configuration command.

The following example configures a IPv6 source address as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv6 source address
```
match message-type

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

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

**Syntax Description**

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

**Command Default**

None

**Command Modes**

Service list configuration.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.3SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Note**

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

**Example**

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

```
Device(config-mdns-sd-sl)# match message-type announcement
```
**match non-client-nrt**

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

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

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

None

**Command Modes**

Class-map

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

None

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

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

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

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

**Syntax Description**

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

**Command Default**

No match criterion is configured.

**Command Modes**

Class-map configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>3E</td>
<td></td>
</tr>
</tbody>
</table>

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

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

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

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

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

This example shows how to create policy maps and define existing class maps for upstream QoS:
Device# configure terminal
Device(config)# policy-map test-avc-up
Device(config-pmap)# class cat-browsing
Device(config-pmap-c)# police 150000
Device(config-pmap-c)# set dscp 12
Device(config-pmap-c)#

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

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

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

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

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

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

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

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

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

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

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

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

```
match service-instance  line
```

**Syntax Description**

- `line`  Regular expression to match the service instance in packets.

**Command Default**

None

**Command Modes**

Service list configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.3SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Example**

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

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

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

```
match service-type  line
```

**Syntax Description**

- `line`  Regular expression to match the service type in packets.

**Command Default**

None

**Command Modes**

Service list configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.3SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Example**

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

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

To configure one or more of the transport fields as a key field for a flow record, use the `match transport` command in flow record configuration mode. To disable the use of one or more of the transport fields as a key field for a flow record, use the `no` form of this command.

#### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>destination-port</code></td>
<td>Configures the transport destination port as a key field.</td>
</tr>
<tr>
<td><code>source-port</code></td>
<td>Configures the transport source port as a key field.</td>
</tr>
</tbody>
</table>

#### Command Default

The transport fields are not configured as a key field.

#### Command Modes

Flow record configuration

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the `match` command.

The following example configures the destination port as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match transport destination-port
```

The following example configures the source port as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match transport source-port
```
match transport

To configure one or more of the transport fields as a key field for a flow record, use the match transport command in flow record configuration mode. To disable the use of one or more of the transport fields as a key field for a flow record, use the no form of this command.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>destination-port</strong></td>
<td>Configures the transport destination port as a key field.</td>
</tr>
<tr>
<td><strong>source-port</strong></td>
<td>Configures the transport source port as a key field.</td>
</tr>
</tbody>
</table>

**Command Default**

The transport fields are not configured as a key field.

**Command Modes**

Flow record configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the match command.

The following example configures the destination port as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match transport destination-port
```

The following example configures the source port as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match transport source-port
```
match transport icmp ipv4

To configure the ICMP IPv4 type field and the code field as key fields for a flow record, use the `match transport icmp ipv4` command in flow record configuration mode. To disable the use of the ICMP IPv4 type field and code field as key fields for a flow record, use the `no` form of this command.

```
match transport icmp ipv4 {code|type}
no match transport icmp ipv4 {code|type}
```

**Syntax Description**
- `code` Configures the IPv4 ICMP code as a key field.
- `type` Configures the IPv4 ICMP type as a key field.

**Command Default**
The ICMP IPv4 type field and the code field are not configured as key fields.

**Command Modes**
Flow record configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the `match` command.

The following example configures the IPv4 ICMP code field as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match transport icmp ipv4 code
```

The following example configures the IPv4 ICMP type field as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match transport icmp ipv4 type
```
match transport icmp ipv4

To configure the ICMP IPv4 type field and the code field as key fields for a flow record, use the `match transport icmp ipv4` command in flow record configuration mode. To disable the use of the ICMP IPv4 type field and code field as key fields for a flow record, use the `no` form of this command.

```
match transport icmp ipv4  {code|type}
no match transport icmp ipv4  {code|type}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>code</code></td>
<td>Configures the IPv4 ICMP code as a key field.</td>
</tr>
<tr>
<td><code>type</code></td>
<td>Configures the IPv4 ICMP type as a key field.</td>
</tr>
</tbody>
</table>

**Command Default**
The ICMP IPv4 type field and the code field are not configured as key fields.

**Command Modes**
Flow record configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the `match` command.

The following example configures the IPv4 ICMP code field as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match transport icmp ipv4 code
```

The following example configures the IPv4 ICMP type field as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match transport icmp ipv4 type
```
match transport icmp ipv6

To configure the ICMP IPv6 type field and the code field as key fields for a flow record, use the `match transport icmp ipv6` command in flow record configuration mode. To disable the use of the ICMP IPv6 type field and code field as key fields for a flow record, use the `no` form of this command.

```
match transport icmp ipv6 {code|type}
no match transport icmp ipv6 {code|type}
```

**Syntax Description**
- `code` Configures the IPv6 ICMP code as a key field.
- `type` Configures the IPv6 ICMP type as a key field.

**Command Default**
The ICMP IPv6 type field and the code field are not configured as key fields.

**Command Modes**
Flow record configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the `match` command.

The following example configures the IPv6 ICMP code field as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match transport icmp ipv6 code
```

The following example configures the IPv6 ICMP type field as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match transport icmp ipv6 type
```
**match transport icmp ipv6**

To configure the ICMP IPv6 type field and the code field as key fields for a flow record, use the `match transport icmp ipv6` command in flow record configuration mode. To disable the use of the ICMP IPv6 type field and code field as key fields for a flow record, use the `no` form of this command.

```
match transport icmp ipv6 {code|type}
no match transport icmp ipv6 {code|type}
```

**Syntax Description**

- `code` Configures the IPv6 ICMP code as a key field.
- `type` Configures the IPv6 ICMP type as a key field.

**Command Default**

The ICMP IPv6 type field and the code field are not configured as key fields.

**Command Modes**

Flow record configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the `match` command.

The following example configures the IPv6 ICMP code field as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match transport icmp ipv6 code
```

The following example configures the IPv6 ICMP type field as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match transport icmp ipv6 type
```
**match user-role**

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

```
match user-role user-role
```

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>config-filter-control-classmap</td>
</tr>
<tr>
<td>Command History</td>
<td></td>
</tr>
<tr>
<td><strong>Release</strong></td>
<td>Modification</td>
</tr>
<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>

**Examples**

The following example shows how to configure a class-map attribute filter criteria:

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

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

```
match username username
no-match username username
```

**Syntax Description**

- **username**
  - Username.

**Command Default**

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

**Command Modes**

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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

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

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

**Examples**

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

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>class</td>
<td>Associates a control class with one or more actions in a control policy.</td>
</tr>
<tr>
<td>policy-map type control subscriber</td>
<td>Defines a control policy for subscriber sessions</td>
</tr>
</tbody>
</table>
match wireless ssid (wireless)

To configure the SSID of the wireless network as a key field for a flow record, use the `match wireless ssid` command in flow record configuration mode. To disable the use of the SSID of the wireless network as a key field for a flow record, use the `no` form of this command.

```
match wireless ssid
no match wireless ssid
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

The SSID of the wireless network is not configured as a key field.

**Command Modes**

Flow record configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.3SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the `match` command.

The following example configures the SSID of the wireless network as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match wireless ssid
```
match wireless ssid (wireless)

To configure the SSID of the wireless network as a key field for a flow record, use the **match wireless ssid** command in flow record configuration mode. To disable the use of the SSID of the wireless network as a key field for a flow record, use the **no** form of this command

```
match wireless ssid
no match wireless ssid
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

The SSID of the wireless network is not configured as a key field.

**Command Modes**

Flow record configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.3SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

The following example configures the SSID of the wireless network as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match wireless ssid
```
**match (access-map configuration)**

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

```
{match ip address \{namenumber\} \{namenumber\} \{namenumber\}...\mac address name \{name\}\{name\}...\}
{no match ip address \{namenumber\} \{namenumber\} \{namenumber\}...\mac address name \{name\}\{name\}...\}
```

**Syntax Description**

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

**Command Default**

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

**Command Modes**

Access-map configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

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

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

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

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

**Examples**

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

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

You can verify your settings by entering the `show vlan access-map` privileged EXEC command.
match (class-map configuration)

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

**Cisco IOS XE Everest 16.5.x and Earlier Releases**

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

**Cisco IOS XE Everest 16.6.x and Later Releases**

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

**Syntax Description**

<table>
<thead>
<tr>
<th>access-group</th>
<th>Specifies an access group.</th>
</tr>
</thead>
<tbody>
<tr>
<td>name acl-name</td>
<td>Specifies the name of an IP standard or extended access control list (ACL) or MAC ACL.</td>
</tr>
<tr>
<td>acl-index</td>
<td>Specifies the number of an IP standard or extended access control list (ACL) or MAC ACL. For an IP standard ACL, the ACL index range is 1 to 99 and 1300 to 1999. For an IP extended ACL, the ACL index range is 100 to 199 and 2000 to 2699.</td>
</tr>
<tr>
<td>class-map class-map-name</td>
<td>Uses a traffic class as a classification policy and specifies a traffic class name to use as the match criterion.</td>
</tr>
<tr>
<td>cos cos-value</td>
<td>Matches a packet on the basis of a Layer 2 class of service (CoS)/Inter-Switch Link (ISL) marking. The cos-value is from 0 to 7. You can specify up to four CoS values in one <code>match cos</code> statement, separated by a space.</td>
</tr>
<tr>
<td>dscp dscp-value</td>
<td>Specifies the parameters for each DSCP value. You can specify a value in the range 0 to 63 specifying the differentiated services code point value.</td>
</tr>
</tbody>
</table>
**ip dscp dscp-list**

Specifies a list of up to eight IP Differentiated Services Code Point (DSCP) values to match against incoming packets. Separate each value with a space. The range is 0 to 63. You also can enter a mnemonic name for a commonly used value.

**ip precedence ip-precedence-list**

Specifies a list of up to eight IP-precedence values to match against incoming packets. Separate each value with a space. The range is 0 to 7. You also can enter a mnemonic name for a commonly used value.

**precedence precedence-value1...value4**

Assigns an IP precedence value to the classified traffic. The range is 0 to 7. You also can enter a mnemonic name for a commonly used value.

**qos-group qos-group-value**

Identifies a specific QoS group value as a match criterion. The range is 0 to 31.

**vlan vlan-id**

Identifies a specific VLAN as a match criterion. The range is 1 to 4094.

**mpls experimental-value**

 Specifies Multi Protocol Label Switching specific values.

**non-client-nrt**

Matches a non-client NRT (non-real-time).

**protocol protocol-name**

 Specifies the type of protocol.

**wlan wlan-id**

Identifies 802.11 specific values.

**Command Default**

No match criteria are defined.

**Command Modes**

Class-map configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE 3.3SE</td>
<td>The <strong>class-map</strong> class-map-name, <strong>cos</strong> cos-value, <strong>qos-group</strong> qos-group-value, and <strong>vlan</strong> vlan-id keywords are added.</td>
</tr>
<tr>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>The <strong>class-map</strong> class-map-name keyword is removed. The <strong>mpls</strong> experimental-value, <strong>non-client-nrt</strong>, <strong>protocol</strong> protocol-name, and <strong>vlan</strong> wlan-id keywords are added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

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

  **Note** The ACL must be an extended named ACL.

- `match ip dscp dscp-list`

- `match ip precedence ip-precedence-list`

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

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

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

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

### Examples

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

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

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

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

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

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

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

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

This example shows how to specify a range of physical ports to which an interface-level class map in a hierarchical policy map applies:
Device(config)# **class-map match-any class4**
Device(config-cmap)# **match cos 4**
Device(config-cmap)# **exit**

You can verify your settings by entering the **show class-map** privileged EXEC command.
To match 802.11 specific values, use the `match wlan user-priority` command in class-map configuration mode. Use the `no` form of this command to return to the default setting.

```plaintext
match wlan user-priority wlan-value [wlan-value] [wlan-value] [wlan-value]
no match wlan user-priority wlan-value [wlan-value] [wlan-value] [wlan-value]
```

**Syntax Description**

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

**Command Default**

None

**Command Modes**

Class-map configuration (config-cmap)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

None

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

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

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

```plaintext
max-bandwidth bandwidth
```

**Syntax Description**

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

**Command Default**

None

**Command Modes**

media-stream

**Command History**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure wireless media-stream bandwidth in Kbps:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless media-stream group doc-grp 224.0.0.0 224.0.0.223
Device(config-media-stream)# max-bandwidth 3500
```
max-through

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

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

**Syntax Description**

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

**Command Default**

10 RAs per VLAN per 10 minutes

**Command Modes**

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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 3.2XE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Example**

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

To configure authentication and authorization method for a mesh AP profile, use the `method` command.

```
method { authentication | authorization } method
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>authentication</code></td>
<td>AAA method for mesh AP authentication.</td>
</tr>
<tr>
<td><code>authorization</code></td>
<td>AAA method for mesh AP authorization.</td>
</tr>
<tr>
<td><code>method</code></td>
<td>Named method list.</td>
</tr>
</tbody>
</table>

**Command Default**

Authentication and authorization method is not configured.

**Command Modes**

`config-wireless-mesh-profile`

**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>

**Example**

The following example shows how to configure authentication for a mesh AP profile:

```
Device # configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device (config)# wireless profile mesh mesh-profile
Device (config-wireless-mesh-profile)# method authentication auth1
```
**method fast**

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

```
method fast [profile profile-name]
```

**Syntax Description**

- `profile-name` Specify the method profile.

**Command Default**

None

**Command Modes**

config-eap-profile

**Command History**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enable EAP Fast method on a EAP profile:

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

To configure mobility sticky anchoring, use the `mobility anchor sticky` command. To disable the sticky anchoring, use the `no` form of the command.

To configure guest anchoring, use the `mobility anchor ip-address` command.

To delete the guest anchor, use the `no` form of the command.

To configure the device as an auto-anchor, use the `mobility anchor` command.

```
mobility anchor {ip-address|sticky}
no mobility anchor {ip-address|sticky}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>sticky</code></td>
<td>The client is anchored to the first switch that it associates.</td>
</tr>
</tbody>
</table>

**Note**

This command is by default enabled and ensures low roaming latency. This ensures that the point of presence for the client does not change when the client joins the mobility domain and roams within the domain.

`ip-address` Configures the IP address for the guest anchor device to this WLAN.

### Command Default

Sticky configuration is enabled by default.

### Command Modes

WLAN Configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE 3.3SE</td>
<td>The auto-anchor configuration required the device IP address to be entered prior to the Cisco IOS XE 3.3SE release; with this release, if no IP address is given, the device itself becomes an anchor; you do not have to explicitly specify the IP address.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The `wlan_id` or `guest_lan_id` must exist and be disabled.
- Auto-anchor mobility is enabled for the WLAN or wired guest LAN when you configure the first mobility anchor.
- Deleting the last anchor disables the auto-anchor mobility feature and resumes normal mobility for new associations.
- Mobility uses the following ports, that are allowed through the firewall:
  - 16666
  - 16667
  - 16668

This example shows how to enable the sticky mobility anchor:

```
Device(config-wlan)# mobility anchor sticky
```
This example shows how to configure guest anchoring:

Device(config-wlan)# mobility anchor 209.165.200.224

This example shows how to configure the device as an auto-anchor:

Device(config-wlan)# mobility anchor
mop enabled

To enable an interface to support the Maintenance Operation Protocol (MOP), use the `mop enabled` command in interface configuration mode. To disable MOP on an interface, use the `no` form of this command.

```
mop enabled
no mop enabled
```

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

**Command Default**
Enabled on Ethernet interfaces and disabled on all other interfaces.

**Command Modes**
Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Examples**
The following example enables MOP for serial interface 0:

```
Router(config)# interface serial 0
Router(config-if)# mop enabled
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mop retransmit-timer</td>
<td>Configures the length of time that the Cisco IOS software waits before sending boot requests again to a MOP server.</td>
</tr>
<tr>
<td>mop retries</td>
<td>Configures the number of times the Cisco IOS software will send boot requests again to a MOP server.</td>
</tr>
<tr>
<td>mop sysid</td>
<td>Enables an interface to send out periodic MOP system identification messages.</td>
</tr>
</tbody>
</table>
mop sysid

To enable an interface to send out periodic Maintenance Operation Protocol (MOP) system identification messages, use the `mop sysid` command in interface configuration mode. To disable MOP message support on an interface, use the `no` form of this command.

```
mop sysid
no mop sysid
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Enabled

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You can still run MOP without having the background system ID messages sent. This command lets you use the MOP remote console, but does not generate messages used by the configurator.

**Examples**

The following example enables serial interface 0 to send MOP system identification messages:

```
Router(config)# interface serial 0
Router(config-if)# mop sysid
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mop device-code</td>
<td>Identifies the type of device sending MOP sysid messages and request program messages.</td>
</tr>
<tr>
<td>mop enabled</td>
<td>Enables an interface to support the MOP.</td>
</tr>
</tbody>
</table>
To configure mesh multicast mode, use the **multicast** command.

```
multicast  { in-only | in-out | regular }
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>in-only</strong></td>
<td>Configures mesh multicast In Mode.</td>
</tr>
<tr>
<td><strong>in-out</strong></td>
<td>Configures mesh multicast In-Out Mode.</td>
</tr>
<tr>
<td><strong>regular</strong></td>
<td>Configures mesh multicast Regular Mode.</td>
</tr>
</tbody>
</table>

### Command Default

in-out

### Command Modes

config-wireless-mesh-profile

### 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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to configure the multicast In Mode for a mesh AP profile:

```
Device # configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device (config)# wireless profile mesh mesh-profile
Device (config-wireless-mesh-profile)# multicast in-only
```
To enable RADIUS Network Admission Control (NAC) support for a WLAN, use the `nac` command. To disable NAC out-of-band support, use the `no` form of this command.

```
nac
no nac
```

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

NAC is disabled.

**Command Modes**

WLAN configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You should enable AAA override before you enable the RADIUS NAC state.

This example shows how to configure RADIUS NAC on the WLAN:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# aaa-override
Device(config-wlan)# nac
```

This example shows how to disable RADIUS NAC on the WLAN:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no nac
Device(config-wlan)# no aaa-override
```
**nas-id option2**

To configure option 2 parameters for a NAS-ID, use the `nas-id option2` command.

```
nas-id option2 {sys-ip |sys-name |sys-mac }
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sys-ip</td>
<td>System IP Address.</td>
</tr>
<tr>
<td>sys-name</td>
<td>System Name.</td>
</tr>
<tr>
<td>sys-mac</td>
<td>System MAC address.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Command Modes</th>
<th>config-aaa-policy</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<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>

**Examples**

The following example shows how to configure the system IP address for the NAS-ID:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless aaa policy profile-name
Device(config-aaa-policy)# nas-id option2 sys-ip
```
network

To configure the network number in decimal notation, use the `network` command.

```
network network-number [ {network-mask | secondary } ]
```

**Syntax Description**

- `ipv4-address` Network number in dotted-decimal notation.
- `network-mask` Network mask or prefix length.
- `secondary` Configure as secondary subnet.

**Command Default**

None

**Command Modes**

dhcp-config

**Command History**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure network number and the mask address:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# ip dhcp pool name
Device(dhcp-config)# network 209.165.200.224 255.255.255.0
```
**nmsp cloud-services enable**

To configure NMSP cloud services, use the **nmsp cloud-services enable** command.

**nmsp cloud-services enable**

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>Global configuration (config)</td>
</tr>
</tbody>
</table>

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enable NMSP cloud services:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# nmsp cloud-services enable
```
**nmsp cloud-services http-proxy**

To configure the proxy for NMSP cloud server, use the `nmsp cloud-services http-proxy` command.

```
nmsp cloud-services http-proxy proxy-server port
```

**Syntax Description**

- `proxy-server` Enter the hostname or the IP address of the proxy server for NMSP cloud services.
- `port` Enter the proxy server port number for NMSP cloud services.

**Command Default**

None

**Command Modes**

Global configuration (config)

**Command History**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure the proxy for NMSP cloud server:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# nmsp cloud-services http-proxy host-name port-number
```
**nmsp cloud-services server token**

To configure the NMSP cloud services server parameters, use the `nmsp cloud-services server token` command.

```
Syntax Description

<table>
<thead>
<tr>
<th>token</th>
<th>Authentication token for the NMSP cloud services.</th>
</tr>
</thead>
</table>

| Command Default | None |

| Command Modes | config |

<table>
<thead>
<tr>
<th>Command History</th>
<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>
<td></td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure the for the NMSP cloud services server parameters:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# nmsp cloud-services server token authentication-token
```
**nmsp cloud-services server url**

To configure NMSP cloud services server URL, use the `nmsp cloud-services server url` command.

```
        nmsp cloud-services server url url
```

**Syntax Description**

- `url`: URL of the NMSP cloud services server.

**Command Default**

None

**Command Modes**

Global configuration (config)

**Command History**

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

**Examples**

The following example shows how to configure a URL for NMSP cloud services server:

```
Device(config)# nmsp cloud-services server url http://www.example.com
```
**nmsp notification interval**

To modify the Network Mobility Services Protocol (NMSP) notification interval value on the controller to address latency in the network, use the **nmsp notification interval** command in global configuration mode.

```
nmsp notification interval { attachment | location | rss { clients | rfid | rogues { ap | client } } }
```

**Syntax Description**

- **attachment** Specifies the time used to aggregate attachment information.
- **location** Specifies the time used to aggregate location information.
- **rssi** Specifies the time used to aggregate RSSI information.
- **clients** Specifies the time interval for clients.
- **rfid** Specifies the time interval for rfid tags.
- **rogues** Specifies the time interval for rogue APs and rogue clients.
- **ap** Specifies the time used to aggregate rogue APs.
- **client** Specifies the time used to aggregate rogue clients.

**Command Default**

No default behavior or values.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

This example shows how to set the NMSP notification interval for the active RFID tags to 25 seconds:

```
Device# configure terminal
Device(config)# nmsp notification-interval rfid 25
Device(config)# end
```

This example shows how to modify NMSP notification intervals for device attachment (connecting to the network or disconnecting from the network) every 10 seconds:

```
Device# configure terminal
Device(config)# nmsp notification-interval attachment 10
Device(config)# end
```

This example shows how to configure NMSP notification intervals for location parameters (location change) every 20 seconds:
Device# configure terminal
Device(config)# nmsp notification-interval location 20
Device(config)# end
**nmsp strong-cipher**

To enable the new ciphers, use the `nmsp strong-cipher` command in global configuration mode. To disable, use the `no` form of this command.

```
no nmsp strong-cipher
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

The new ciphers are not enabled.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.2(2)E</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `nmsp strong-cipher` command enables strong ciphers for new Network Mobility Service Protocol (NMSP) connections.

**Note**

The existing NMSP connections will use the default cipher.

**Examples**

The following example shows how to enable a strong-cipher for NMSP:

```
Device> enable
Device> configure terminal
Device(config)# nmsp strong-cipher
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>show nmsp status</strong></td>
<td>Displays the status of active NMSP connections.</td>
</tr>
</tbody>
</table>
office-extend

To enable the OfficeExtend AP mode for a FlexConnect AP, use the **office-extend** command.

---

**office-extend**

Command Default  
None

Command Modes  
config-wireless-flex-profile

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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

---

**Examples**

The following example shows how to enable the OfficeExtend AP mode for a FlexConnect AP:

Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless profile flex flex-profile-name
Device(config-wireless-flex-profile)# office-extend
option

To configure optional data parameters for a flow exporter, use the `option` command in flow exporter configuration mode. To remove optional data parameters for a flow exporter, use the `no` form of this command.

```
option {exporter-stats|interface-table|sampler-table} [timeout seconds]
no option {exporter-stats|interface-table|sampler-table}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>exporter-stats</td>
<td>Configures the exporter statistics option for flow exporters.</td>
</tr>
<tr>
<td>interface-table</td>
<td>Configures the interface table option for flow exporters.</td>
</tr>
<tr>
<td>sampler-table</td>
<td>Configures the export sampler table option for flow exporters.</td>
</tr>
<tr>
<td>timeout seconds</td>
<td>(Optional) Configures the option resend time in seconds for flow exporters. The range is 1 to 86400. The default is 600.</td>
</tr>
</tbody>
</table>

### Command Default

The timeout is 600 seconds. All other optional data parameters are not configured.

### Command Modes

Flow exporter configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE 3.3SE</td>
<td>The <code>application-table</code> and <code>usermac-table</code> keywords were added.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The `option exporter-stats` command causes the periodic sending of the exporter statistics, including the number of records, bytes, and packets sent. This command allows the collector to estimate packet loss for the export records it receives. The optional timeout alters the frequency at which the reports are sent.

The `option interface-table` command causes the periodic sending of an options table, which allows the collector to map the interface SNMP indexes provided in the flow records to interface names. The optional timeout can alter the frequency at which the reports are sent.

The `option sampler-table` command causes the periodic sending of an options table, which details the configuration of each sampler and allows the collector to map the sampler ID provided in any flow record to a configuration that it can use to scale up the flow statistics. The optional timeout can alter the frequency at which the reports are sent.

To return this command to its default settings, use the `no option` or `default option` flow exporter configuration command.

The following example shows how to enable the periodic sending of the sampler option table, which allows the collector to map the sampler ID to the sampler type and rate:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# option sampler-table
```

The following example shows how to enable the periodic sending of the exporter statistics, including the number of records, bytes, and packets sent:
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# option exporter-stats

The following example shows how to enable the periodic sending of an options table, which allows the collector to map the interface SNMP indexes provided in the flow records to interface names:

Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# option interface-table
packet-capture

To enable packet capture on the AP profile, use the packet-capture command.

**packet-capture profile-name**

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>config-ap-profile</td>
</tr>
<tr>
<td>Command History</td>
<td>Release</td>
</tr>
<tr>
<td></td>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure packet capture on the AP profile:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# ap profile demo-profile-name
Device(config-ap-profile)# packet capture demo-profile
```
### parameter-map type subscriber attribute-to-service

To configure parameter map type and name, use the `parameter-map type subscriber attribute-to-service` command.

```
parameter-map type subscriber attribute-to-service parameter-map-name
```

#### Syntax Description

- **attribute-to-service** Name the attribute to service.
- **parameter-map-name** Name of the parameter map. The map name is limited to 33 characters.

#### Command Default

None

#### Command Modes

Global configuration (config)

#### Command History

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

#### Examples

The following example shows how to configure parameter map type and name:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# parameter-map type subscriber attribute-to-service parameter-map-name
```
parameter-map type umbrella global

To configure an umbrella global parameter map, use the `parameter-map type umbrella global` command.

**Command Default**
None

**Command Modes**
Global configuration (config)

**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>

**Usage Guidelines**
As a prerequisite, you need to create a regex parameter map. In the example section, `dns_wl` is the sample parameter map name.

**Example**
This example shows how to configure an umbrella global parameter map:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config) 参数 type umbrella global
Device(config-profile)# token 57CC80106C087FB1B2A7BAB4F2F4373C00247166
Device(config-profile)# local-domain dns_wl
Device(config-profile)# end
```
peer-blocking

To configure peer-to-peer blocking on a WLAN, use the **peer-blocking** command. To disable peer-to-peer blocking, use the **no** form of this command.

**peer-blocking {drop|forward-upstream}**

**no peer-blocking**

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>drop</td>
<td>Specifies the device to discard the packets.</td>
</tr>
<tr>
<td>forward-upstream</td>
<td>Specifies the packets to be forwarded on the upstream VLAN. The device next in the hierarchy to the device decides what action to take regarding the packets.</td>
</tr>
</tbody>
</table>

**Command Default**

Peer blocking is disabled.

**Command Modes**

WLAN configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

This example shows how to enable the drop and forward-upstream options for peer-to-peer blocking:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# peer-blocking drop
Device(config-wlan)# peer-blocking forward-upstream
```

This example shows how to disable the drop and forward-upstream options for peer-to-peer blocking:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no peer-blocking drop
Device(config-wlan)# no peer-blocking forward-upstream
```
To configure media stream admission policy, use the `policy` command.

```
policy {admit | deny}
```

**Syntax Description**

- **admit**: Allows traffic for a media stream group.
- **deny**: Denies traffic for a media stream group.

**Command Default**
None

**Command Modes**
media-stream

**Command History**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to allow traffic for a media stream group:

```
Device # configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless media-stream group ms-group 224.0.0.0 224.0.0.223
Device(media-stream)# policy admit
```
police

To define a policer for classified traffic, use the `police` command in policy-map class configuration mode. Use the `no` form of this command to remove an existing policer.

```
police rate-bps burst-byte [conform-action transmit]
no police rate-bps burst-byte [conform-action transmit]
```

**Syntax Description**

- `rate-bps`: Specify the average traffic rate in bits per second (b/s). The range is 1000000 to 1000000000.
- `burst-byte`: Specify the normal burst size in bytes. The range is 8000 to 1000000.
- `conform-action transmit`: (Optional) When less than the specified rate, specify that the switch transmits the packet.

**Command Default**

No policers are defined.

**Command Modes**

Policy-map class configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

A policer defines a maximum permissible rate of transmission, a maximum burst size for transmissions, and an action to take if either maximum is exceeded.

When configuring hierarchical policy maps, you can only use the `police` policy-map command in a secondary interface-level policy map.

The port ASIC device, which controls more than one physical port, supports 256 policers on the switch (255 user-configurable policers plus 1 policer reserved for internal use). The maximum number of configurable policers supported per port is 63. Policers are allocated on demand by the software and are constrained by the hardware and ASIC boundaries. You cannot reserve policers per port. There is no guarantee that a port will be assigned to any policer.

To return to policy-map configuration mode, use the `exit` command. To return to privileged EXEC mode, use the `end` command.

**Examples**

This example shows how to configure a policer that transmits packets if traffic is less than 1 Mb/s average rate with a burst size of 20 KB. There is no packet modification.

```
Device(config)# class-map class1
Device(config-cmap)# exit
Device(config)# policy-map policy1
Device(config-pmap)# class class1
Device(config-pmap-c)# police 1000000 20000 conform-action transmit
Device(config-pmap-c)# exit
```
This example shows how to configure a policer that transmits packets if traffic is less than 1 Mb/s average rate with a burst size of 20 KB. There is no packet modification. This example uses an abbreviated syntax:

```
Device(config)# class-map class1
Device(config-cmap)# exit
Device(config)# policy-map policy1
Device(config-pmap)# class class1
Device(config-pmap-c)# police 1m 20000 conform-action transmit
Device(config-pmap-c)# exit
```

This example shows how to configure a policer, which marks down the DSCP values with the values defined in policed-DSCP map and sends the packet:

```
Device(config)# policy-map policy2
Device(config-pmap)# class class2
Device(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
Device(config-pmap-c)# exit
```

You can verify your settings by entering the `show policy-map` privileged EXEC command.
policy-tag

To map a policy tag to the AP, use the `policy-tag` command.

```
policy-tag policy-tag-name
```

**Syntax Description**

- `policy-tag-name`: Name of the policy tag.

**Command Default**

None

**Command Modes**

config-ap-tag

**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>

**Usage Guidelines**

The AP will disconnect and rejoin after running this command.

**Example**

The following example shows how to configure a policy tag:

```
Device(config-ap-tag)# policy-tag policytag1
```
policy-map

To create or modify a policy map that can be attached to multiple physical ports or switch virtual interfaces (SVIs) and to enter policy-map configuration mode, use the **policy-map** command in global configuration mode. Use the **no** form of this command to delete an existing policy map and to return to global configuration mode.

```
policy-map policy-map-name
no policy-map policy-map-name
```

**Syntax Description**

- `policy-map-name` Name of the policy map.

**Command Default**

No policy maps are defined.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

After entering the **policy-map** command, you enter policy-map configuration mode, and these configuration commands are available:

- **class**—Defines the classification match criteria for the specified class map.
- **description**—Describes the policy map (up to 200 characters).
- **exit**—Exits policy-map configuration mode and returns you to global configuration mode.
- **no**—Removes a previously defined policy map.
- **sequence-interval**—Enables sequence number capability.

To return to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

Before configuring policies for classes whose match criteria are defined in a class map, use the **policy-map** command to specify the name of the policy map to be created, added to, or modified. Entering the **policy-map** command also enables the policy-map configuration mode in which you can configure or modify the class policies for that policy map.

You can configure class policies in a policy map only if the classes have match criteria defined for them. To configure the match criteria for a class, use the **class-map** global configuration and **match** class-map configuration commands. You define packet classification on a physical-port basis.

Only one policy map per ingress port is supported. You can apply the same policy map to multiple physical ports.

You can apply a nonhierarchical policy maps to physical ports. A nonhierarchical policy map is the same as the port-based policy maps in the device.

A hierarchical policy map has two levels in the format of a parent-child policy. The parent policy cannot be modified but the child policy (port-child policy) can be modified to suit the QoS configuration.
In VLAN-based QoS, a service policy is applied to an SVI interface.

Note

Not all MQC QoS combinations are supported for wired ports. For information about these restrictions, see chapters "Restrictions for QoS on Wired Targets" in the QoS configuration guide.

Examples

This example shows how to create a policy map called policy1. When attached to the ingress port, it matches all the incoming traffic defined in class1, sets the IP DSCP to 10, and polices the traffic at an average rate of 1 Mb/s and bursts at 20 KB. Traffic less than the profile is sent.

```
Device(config)# policy-map policy1
Device(config-pmap)# class class1
Device(config-pmap-c)# set dscp 10
Device(config-pmap-c)# police 1000000 20000 conform-action transmit
Device(config-pmap-c)# exit
```

This example show you how to configure hierarchical polices:

```
Device(config)# configure terminal
Device(config)# class-map c1
Device(config-cmap)# exit

Device(config)# class-map c2
Device(config-cmap)# exit

Device(config)# policy-map child
Device(config-pmap)# class c1
Device(config-pmap-c)# priority level 1
Device(config-pmap-c)# police rate percent 20 conform-action transmit exceed action drop
Device(config-pmap-c-police)# exit
Device(config-pmap-c)# exit

Device(config-pmap)# class c2
Device(config-pmap-c)# bandwidth 20000
Device(config-pmap-c)# exit

Device(config-pmap)# class class-default
Device(config-pmap-c)# bandwidth 20000
Device(config-pmap-c)# exit
Device(config-pmap)# exit

Device(config)# policy-map parent
Device(config-pmap)# class class-default
Device(config-pmap-c)# shape average 1000000
Device(config-pmap-c)# service-policy child
Device(config-pmap-c)# end
```

This example shows how to delete a policy map:

```
Device(config)# no policy-map policymap2
```

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

To create or modify a policy map that can be attached to multiple physical ports or switch virtual interfaces (SVIs) and to enter policy-map configuration mode, use the `policy-map` command in global configuration mode. Use the `no` form of this command to delete an existing policy map and to return to global configuration mode.

```
policy-map policy-map-name
no policy-map policy-map-name
```

**Syntax Description**

- `policy-map-name` Name of the policy map.

**Command Default**

No policy maps are defined.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

After entering the `policy-map` command, you enter policy-map configuration mode, and these configuration commands are available:

- `class`—Defines the classification match criteria for the specified class map.
- `description`—Describes the policy map (up to 200 characters).
- `exit`—Exits policy-map configuration mode and returns you to global configuration mode.
- `no`—Removes a previously defined policy map.
- `sequence-interval`—Enables sequence number capability.

To return to global configuration mode, use the `exit` command. To return to privileged EXEC mode, use the `end` command.

Before configuring policies for classes whose match criteria are defined in a class map, use the `policy-map` command to specify the name of the policy map to be created, added to, or modified. Entering the `policy-map` command also enables the policy-map configuration mode in which you can configure or modify the class policies for that policy map.

You can configure class policies in a policy map only if the classes have match criteria defined for them. To configure the match criteria for a class, use the `class-map` global configuration and `match` class-map configuration commands. You define packet classification on a physical-port basis.

Only one policy map per ingress port is supported. You can apply the same policy map to multiple physical ports.

You can apply a nonhierarchical policy maps to physical ports. A nonhierarchical policy map is the same as the port-based policy maps in the device.

A hierarchical policy map has two levels in the format of a parent-child policy. The parent policy cannot be modified but the child policy (port-child policy) can be modified to suit the QoS configuration.
In VLAN-based QoS, a service policy is applied to an SVI interface.

**Note**

Not all MQC QoS combinations are supported for wired ports. For information about these restrictions, see chapters "Restrictions for QoS on Wired Targets" in the QoS configuration guide.

### Examples

This example shows how to create a policy map called `policy1`. When attached to the ingress port, it matches all the incoming traffic defined in class1, sets the IP DSCP to 10, and polices the traffic at an average rate of 1 Mb/s and bursts at 20 KB. Traffic less than the profile is sent.

```
Device(config)# policy-map policy1
Device(config-pmap)# class class1
Device(config-pmap-c)# set dscp 10
Device(config-pmap-c)# police 1000000 20000 conform-action transmit
Device(config-pmap-c)# exit
```

This example show you how to configure hierarchical polices:

```
Device# configure terminal
Device(config)# class-map c1
Device(config-cmap)# exit

Device(config)# class-map c2
Device(config-cmap)# exit

Device(config)# policy-map child
Device(config-pmap)# class c1
Device(config-pmap-c)# priority level 1
Device(config-pmap-c)# police rate percent 20 conform-action transmit exceed action drop
Device(config-pmap-c-police)# exit

Device(config-pmap-c)# class c2
Device(config-pmap-c)# bandwidth 20000
Device(config-pmap-c)# exit

Device(config-pmap-c)# class class-default
Device(config-pmap-c)# bandwidth 20000
Device(config-pmap-c)# exit
Device(config-pmap-c)# exit

Device(config)# policy-map parent
Device(config-pmap)# class class-default
Device(config-pmap-c)# shape average 1000000
Device(config-pmap-c)# service-policy child
Device(config-pmap-c)# end
```

This example shows how to delete a policy map:

```
Device(config)# no policy-map policymap2
```

You can verify your settings by entering the `show policy-map` privileged EXEC command.
To configure the port number to use when configuring the custom application, use the `port` command.

```
port  port-no
```

**Syntax Description**
- `port-no` Port number.

**Command Default**
None

**Command Modes**
config-custom

**Command History**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure the port number to use when configuring the custom application:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# ip nbar custom custom-protocol http host host-string
Device(config-custom)# http host hostname
Device(config-custom)# port port-no
```
**priority priority-value**

To configure media stream priority, use the **priority priority-value** command.

```
priority priority-value
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>priority-value</td>
<td>Media stream priority value. Valid range is 1 to 8, with 1 being lowest priority and 8 being highest priority.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
</table>

**Command Modes**

- config-media-stream

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to set the media stream priority value to the highest, that is 8:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless media-stream group my-media-group 224.0.0.0 224.0.0.223
Device(config-media-stream)# priority 8
```
priority-queue

To enable the egress expedite queue on a port, use the **priority-queue** command in interface configuration mode. Use the **no** form of this command to return to the default setting.

**priority-queue out**
**no priority-queue out**

### Syntax Description

- **at** Enable the egress expedite queue.

### Command Default

The egress expedite queue is disabled.

### Command Modes

Interface configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

When you configure the **priority-queue out** command, the shaped round robin (SRR) weight ratios are affected because there is one fewer queue participating in SRR. This means that weight1 in the **srr-queue bandwidth shape** or the **srr-queue bandwidth share** interface configuration command is ignored (not used in the ratio calculation). The expedite queue is a priority queue, and it is serviced until empty before the other queues are serviced.

Follow these guidelines when the expedite queue is enabled or the egress queues are serviced based on their SRR weights:

- If the egress expedite queue is enabled, it overrides the SRR shaped and shared weights for queue 1.
- If the egress expedite queue is disabled and the SRR shaped and shared weights are configured, the shaped mode overrides the shared mode for queue 1, and SRR services this queue in shaped mode.
- If the egress expedite queue is disabled and the SRR shaped weights are not configured, SRR services the queue in shared mode.

### Examples

This example shows how to enable the egress expedite queue when the SRR weights are configured. The egress expedite queue overrides the configured SRR weights.

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# srr-queue bandwidth shape 25 0 0 0
Device(config-if)# srr-queue bandwidth share 30 20 25 25
Device(config-if)# priority-queue out
```

This example shows how to disable the egress expedite queue after the SRR shaped and shared weights are configured. The shaped mode overrides the shared mode.

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# srr-queue bandwidth shape 25 0 0 0
Device(config-if)# srr-queue bandwidth share 30 20 25 25
Device(config-if)# no priority-queue out
```
You can verify your settings by entering the `show mls qos interface interface-id queueing` or the `show running-config` privileged EXEC command.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show mls qos interface queueing</code></td>
<td>Displays the queueing strategy (SRR, priority queueing), the weights corresponding to the queues, and the CoS-to-egress-queue map.</td>
</tr>
<tr>
<td><code>srr-queue bandwidth shape</code></td>
<td>Assigns the shaped weights and enables bandwidth shaping on the four egress queues mapped to a port.</td>
</tr>
<tr>
<td><code>srr-queue bandwidth share</code></td>
<td>Assigns the shared weights and enables bandwidth sharing on the four egress queues mapped to a port.</td>
</tr>
</tbody>
</table>
priority

To assign priority to a class of traffic belonging to a policy map, use the `priority` command in policy-map class configuration mode. To remove a previously specified priority for a class, use the `no` form of this command.

```
priority [Kbps [burst -in-bytes] | level level-value [Kbps [burst -in-bytes]]] | percent percentage
no priority [Kb/s [burst -in-bytes] | level level-value [Kb/s [burst -in-bytes]]] | percent percentage
```

**Syntax Description**

- **Kbps**
  - (Optional) Guaranteed allowed bandwidth, in kilobits per second (kbps), for the priority traffic. The amount of guaranteed bandwidth varies according to the interface and platform in use. Beyond the guaranteed bandwidth, the priority traffic will be dropped in the event of congestion to ensure that the nonpriority traffic is not starved. The value must be between 1 and 2,000,000 kbps.

- **burst -in-bytes**
  - (Optional) Burst size in bytes. The burst size configures the network to accommodate temporary bursts of traffic. The default burst value, which is computed as 200 milliseconds of traffic at the configured bandwidth rate, is used when the burst argument is not specified. The range of the burst is from 32 to 2000000 bytes.

- **level level-value**
  - (Optional) Assigns priority level. Available values for `level-value` are 1 and 2. Level 1 is a higher priority than Level 2. Level 1 reserves bandwidth and goes first, so latency is very low.

- **percent percentage**
  - (Optional) Specifies the amount of guaranteed bandwidth to be specified by the percent of available bandwidth.

**Command Default**

No priority is set.

**Command Modes**

Policy-map class configuration (config-pmap-c)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE 3.3SE</td>
<td>The Kbps, burst -in-bytes, and percent percentage keywords were added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The priority command allows you to set up classes based on a variety of criteria (not just User Datagram Ports [UDP] ports) and assign priority to them, and is available for use on serial interfaces and permanent virtual circuits (PVCs). A similar command, the `ip rtp priority` command, allows you to stipulate priority flows based only on UDP port numbers and is not available for PVCs.

The bandwidth and priority commands cannot be used in the same class, within the same policy map. However, these commands can be used together in the same policy map.
Within a policy map, you can give one or more classes priority status. When multiple classes within a single policy map are configured as priority classes, all traffic from these classes is queued to the same, single, priority queue.

When the policy map containing class policy configurations is attached to the interface to stipulate the service policy for that interface, available bandwidth is assessed. If a policy map cannot be attached to a particular interface because of insufficient interface bandwidth, the policy is removed from all interfaces to which it was successfully attached.

**Example**

The following example shows how to configure the priority of the class in policy map policy1:

```plaintext
Device(config)# class-map cm1
Device(config-cmap)# match precedence 2
Device(config-cmap)# exit

Device(config)# class-map cm2
Device(config-cmap)# match dscp 30
Device(config-cmap)# exit

Device(config)# policy-map policy1
Device(config-pmap)# class cm1
Device(config-pmap-c)# priority level 1
Device(config-pmap-c)# police 1m
Device(config-pmap-c)# exit
Device(config-pmap-c)# exit

Device(config)# policy-map policy1
Device(config-pmap)# class cm2
Device(config-pmap-c)# priority level 2
Device(config-pmap-c)# police 1m
```
**protocol (IPv6 snooping)**

To specify that addresses should be gleaned with Dynamic Host Configuration Protocol (DHCP) or Neighbor Discovery Protocol (NDP), or to associate the protocol with an IPv6 prefix list, use the `protocol` command. To disable address gleaning with DHCP or NDP, use the `no` form of the command.

```
protocol { dhcp | ndp }
no protocol { dhcp | ndp }
```

**Syntax Description**

- `dhcp` Specifies that addresses should be gleaned in Dynamic Host Configuration Protocol (DHCP) packets.
- `ndp` Specifies that addresses should be gleaned in Neighbor Discovery Protocol (NDP) packets.

**Command Default**

Snooping and recovery are attempted using both DHCP and NDP.

**Command Modes**

IPv6 snooping configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If an address does not match the prefix list associated with DHCP or NDP, then control packets will be dropped and recovery of the binding table entry will not be attempted with that protocol.

- Using the `no protocol { dhcp | ndp }` command indicates that a protocol will not be used for snooping or gleaning.
- If the `no protocol dhcp` command is used, DHCP can still be used for binding table recovery.
- Data glean can recover with DHCP and NDP, though destination guard will only recovery through DHCP.

This example shows how to define an IPv6 snooping policy name as `policy1`, place the switch in IPv6 snooping policy configuration mode, and configure the port to use DHCP to glean addresses:

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# protocol dhcp
```
qos queue-softmax-multiplier

To increase the value of softmax buffer, use the qos queue-softmax-multiplier command in the global configuration mode.

```
qos queue-softmax-multiplier  range-of-multiplier
no  qos queue-softmax-multiplier  range-of-multiplier
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>range-of-multiplier</td>
<td>You can specify a value in the range of 100 to 1200. The default value is 100.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

Global configuration (config)

**Command History**

**Usage Guidelines**

This command would take effect only on the ports where a policy-map is attached. If configured as 1200, the softmax for non-priority queues and non-primary priority queue (!=level 1) are multiplied by 12 with their default values. This command is not applicable for priority queue level 1.

Note: The command would only take effect on the ports where a policy-map is attached.
qos video

To configure over-the-air QoS class to video only, use the qos video command.

```plaintext
qos video
```

**Command Default**

None

**Command Modes**

config-media-stream

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure over-the-air QoS class to video only:

```plaintext
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless media-stream group my-media-group 224.0.0.0 224.0.0.223
Device(config-media-stream)# qos video
```
**qos wireless-default untrust**

To configure the default trust behavior to untrust wireless packets, use the `qos wireless-default untrust` command. To configure the default trust behavior of wireless traffic to trust, use the `no` form of the command.

```
qos wireless-default-untrust
no qos wireless-default-untrust
```

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

**Command Default**
By default, the wireless traffic is untrusted.

To check the trust behavior on the device, use the `show running-config | sec qos` or the `show run | include untrust` command.

**Command Modes**
Configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.3SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

---

**Note**
The default trust behavior of wireless traffic was untrusted in the Cisco IOS XE 3.2 SE release.

---

**Note**
If you upgrade from Cisco IOS XE 3.2 SE Release to a later release, the default behavior of the wireless traffic is still untrusted. In this situation, you can use the `no qos wireless-default untrust` command to enable trust behavior for wireless traffic. However, if you install Cisco IOS XE 3.3 SE or a later release on the device, the default QoS behavior for wireless traffic is trust. Starting with Cisco IOS XE 3.3 SE Release and later, the packet markings are preserved in both egress and ingress directions for new installations (not upgrades) for wireless traffic.

The Cisco IOS XE 3.2 Release supported different trust defaults for wired and wireless ports. The trust default for wired ports was the same as for this software release. For wireless ports, the default system behavior was non-trust, which meant that when the device came up, all markings for the wireless ports were defaulted to zero and no traffic received priority treatment. For compatibility with an existing wired device, all traffic went to the best-effort queue by default. The access point performed priority queuing by default. In the downstream direction, the access point maintained voice, video, best-effort, and background queues for queuing. The access selected the queuing strategy based on the 802.11e tag information. By default, the access point treated all wireless packets as best effort.

The following command changes the default behavior for trusting wireless traffic to untrust.

```
Device(config)# qos wireless-default-untrust
```
queue-buffers ratio

To configure the queue buffer for the class, use the queue-buffers ratio command in policy-map class configuration mode. Use the no form of this command to remove the ratio limit.

```
queue-buffers ratio  ratio limit
no queue-buffers ratio  ratio limit
```

**Syntax Description**

- `ratio limit` (Optional) Configures the queue buffer for the class. Enter the queue buffers ratio limit (0-100).

**Command Default**

No queue buffer for the class is defined.

**Command Modes**

Policy-map class configuration (config-pmap-c)

**Command History**

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

**Usage Guidelines**

Either the **bandwidth**, shape, or priority command must be used before using this command. For more information about these commands, see Cisco IOS Quality of Service Solutions Command Reference available on Cisco.com.

The allows you to allocate buffers to queues. If buffers are not allocated, then they are divided equally amongst all queues. You can use the queue-buffer ratio to divide it in a particular ratio. The buffers are soft buffers because Dynamic Threshold and Scaling (DTS) is active on all queues by default.

**Example**

The following example sets the queue buffers ratio to 10 percent:

```
Device(config)# policy-map policy_queuebuf01
Device(config-pmap)# class-map class_queuebuf01
Device(config-cmap)# exit
Device(config)# policy policy_queuebuf01
Device(config-pmap)# class class_queuebuf01
Device(config-pmap-c)# bandwidth percent 80
Device(config-pmap-c)# queue-buffers ratio 10
Device(config-pmap-c)# end
```

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

To specify or modify the maximum number of packets the queue can hold for a class policy configured in a policy map, use the `queue-limit` policy-map class configuration command. To remove the queue packet limit from a class, use the `no` form of this command.

```
queue-limit queue-limit-size [{packets}] {cos cos-value|dscp dscp-value} percent percentage-of-packets
no queue-limit queue-limit-size [{packets}] {cos cos-value|dscp dscp-value} percent percentage-of-packets
```

**Syntax Description**

- `queue-limit-size` The maximum size of the queue. The maximum varies according to the optional unit of measure keyword specified (bytes, ms, us, or packets).
- `cos cos-value` Specifies parameters for each cos value. CoS values are from 0 to 7.
- `dscp dscp-value` Specifies parameters for each DSCP value. You can specify a value in the range 0 to 63 specifying the differentiated services code point value for the type of queue limit.
- `percent percentage-of-packets` A percentage in the range 1 to 100 specifying the maximum percentage of packets that the queue for this class can accumulate.

**Command Default**
None

**Command Modes**
Policy-map class configuration (policy-map-c)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Although visible in the command line help-strings, the `packets` unit of measure is not supported; use the `percent` unit of measure.

- **Note**

  This command is supported only on wired ports in the egress direction.

  Weighted fair queuing (WFQ) creates a queue for every class for which a class map is defined. Packets satisfying the match criteria for a class accumulate in the queue reserved for the class until they are sent, which occurs when the queue is serviced by the fair queuing process. When the maximum packet threshold you defined for the class is reached, queuing of any further packets to the class queue causes tail drop.

  You use queue limits to configure Weighted Tail Drop (WTD). WTD ensures the configuration of more than one threshold per queue. Each class of service is dropped at a different threshold value to provide for QoS differentiation.
You can configure the maximum queue thresholds for the different subclasses of traffic, that is, DSCP and CoS and configure the maximum queue thresholds for each subclass.

**Example**

The following example configures a policy map called port-queue to contain policy for a class called dscp-1. The policy for this class is set so that the queue reserved for it has a maximum packet limit of 20 percent:

```
Device(config)# policy-map policy11
Device(config-pmap)# class dscp-1
Device(config-pmap-c)# bandwidth percent 20
Device(config-pmap-c)# queue-limit dscp 1 percent 20
```
queue-set

To map a port to a queue set, use the `queue-set` command in interface configuration mode. Use the no form of this command to return to the default setting.

```
queue-set  qset-id
no queue-set  qset-id
```

**Syntax Description**

`qset-id` Queue-set ID. Each port belongs to a queue set, which defines all the characteristics of the four egress queues per port. The range is 1 to 2.

**Command Default**

The queue set ID is 1.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to map a port to queue-set 2:

```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# queue-set 2
```

You can verify your settings by entering the `show mls qos interface [interface-id] buffers` privileged EXEC command.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mls qos queue-set output buffers</td>
<td>Allocates buffers to a queue set.</td>
</tr>
<tr>
<td>mls qos queue-set output threshold</td>
<td>Configures the weighted tail-drop (WTD) thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue set.</td>
</tr>
</tbody>
</table>
radius server

To configure the RADIUS server, use the `radius server` command in global configuration mode.

```
radius server  server-name
```

**Syntax Description**

| server-name | RADIUS server name. |

**Command Default**

None

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

None

The following example shows how to configure a radius server:

```
Device(config)# radius server ISE
```
range

To configure range from MAP to RAP bridge, use the `range` command.

```
range  range-in-feet
```

**Syntax Description**

- `range-in-feet` Configure the range value in terms of feet. Valid range is from 150 feet to 132000 feet.

**Command Default**

1200

**Command Modes**

config-wireless-mesh-profile

**Command History**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure range from MAP to RAP bridge for a mesh AP profile:

```
Device # configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device (config)# wireless profile mesh mesh-profile
Device (config-wireless-mesh-profile)# range 300
```
reanchor class

To configure classmap with protocols for the selective reanchoring feature, use the `reanchor class` command.

```
reanchor class class-name
```

Syntax Description

- `class-name`: AVC reanchor class name.

Command Default

None

Command Modes

- `config-wireless-policy`

Command History

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

Examples

The following example shows how to configure an AVC reanchor class name:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless profile policy default-policy-profile
Device(config-wireless-policy)# reanchor class AVC-Reanchor-Class
```
record wireless avc basic

To apply the wireless avc basic AVC flow record to a flow monitor, use the record wireless avc basic command.

record wireless avc basic

Command Default
None

Command Modes
config-flow-monitor

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

Usage Guidelines
This command specifies the basic wireless AVC template. When you are configuring AVC, you will need to create a flow monitor using the record wireless avc basic command.

Examples
The following example shows how to apply the wireless avc basic AVC flow record to a flow monitor named test-flow:

Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# flow monitor test-flow
Device(config-flow-monitor)# record wireless avc basic
# redundancy revertive

To set redundancy model as revertive, use the **redundancy revertive** command.

## Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>This command has no keywords or arguments.</td>
</tr>
</tbody>
</table>

## Command Default

<table>
<thead>
<tr>
<th>Command Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
</tr>
</tbody>
</table>

## Command Modes

<table>
<thead>
<tr>
<th>Command Modes</th>
</tr>
</thead>
<tbody>
<tr>
<td>EoGRE domain configuration</td>
</tr>
</tbody>
</table>

## Command History

<table>
<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>

## Example

This example shows how to set redundancy model as revertive:

```
Device(config-eogre-domain)# redundancy revertive
```
redirect

To configure a redirect to an external portal, use the **redirect** command.

```
redirect {for-login |on-failure |on-success }redirect-url-name
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>for-login</td>
<td>To login, redirect to this URL.</td>
</tr>
<tr>
<td>on-failure</td>
<td>If login fails, redirect to this URL.</td>
</tr>
<tr>
<td>on-success</td>
<td>If login is successful, redirect to this URL.</td>
</tr>
<tr>
<td>redirect-url-name</td>
<td>Redirect URL name.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

config-params-parameter-map

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure an redirect to an external IPv4 URL to login:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# parameter-map type webauth parameter-name
Device(config-params-parameter-map)# redirect for-login cisco.com
```
**redirect portal**

To configure external IPv4 or IPv6 portal, use the `redirect portal` command.

```
redirect portal {ipv4 | ipv6} ip-addr
```

**Syntax Description**
- `ipv4` IPv4 portal address
- `ipv6` IPv6 portal address

**Command Default**
None

**Command Modes**
config-params-parameter-map

**Command History**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure an external IPv4 portal address:

Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# parameter-map type webauth parameter-name
Device(config-params-parameter-map)# redirect portal ipv4 192.168.1.100
remote-span

To configure a VLAN as a Remote Switched Port Analyzer (RSPAN) VLAN, use the remote-span command in VLAN configuration mode on the switch stack or on a standalone switch. To remove the RSPAN designation from the VLAN, use the no form of this command.

```
remote-span
no remote-span
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No RSPAN VLANs are defined.

**Command Modes**

VLAN configuration (config-VLAN)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If VLAN Trunking Protocol (VTP) is enabled, the RSPAN feature is propagated by VTP for VLAN IDs that are lower than 1005. If the RSPAN VLAN ID is in the extended range, you must manually configure intermediate switches (those in the RSPAN VLAN between the source switch and the destination switch).

Before you configure the RSPAN remote-span command, use the vlan (global configuration) command to create the VLAN.

The RSPAN VLAN has these characteristics:

- No MAC address learning occurs on it.
- RSPAN VLAN traffic flows only on trunk ports.
- Spanning Tree Protocol (STP) can run in the RSPAN VLAN, but it does not run on RSPAN destination ports.

When an existing VLAN is configured as an RSPAN VLAN, the VLAN is first deleted and then recreated as an RSPAN VLAN. Any access ports are made inactive until the RSPAN feature is disabled.

This example shows how to configure a VLAN as an RSPAN VLAN:

```
Device(config)# vlan 901
Device(config-vlan)# remote-span
```

This example shows how to remove the RSPAN feature from a VLAN:

```
Device(config)# vlan 901
Device(config-vlan)# no remote-span
```

You can verify your settings by entering the show vlan remote-span user EXEC command.
remote-lan

To map an RLAN policy profile to an RLAN profile, use the remote-lan command.

```
remote-lan remote-lan-profile-name policy rlan-policy-profile-name port-id port-id
```

**Syntax Description**

- `remote-lan-profile-name`: Remote LAN profile name.
- `rlan-policy-profile-name`: Remote LAN policy profile name.
- `port-id`: Port ID.

**Command Default**

None

**Command Modes**

Global configuration (config)

**Command History**

<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>

**Example**

This example shows how to map an RLAN policy profile to an RLAN profile:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless tag policy remote-lan-policy-tag
Device(config-policy-tag)# remote-lan rlan_profile_name policy rlan_policy_profile port-id 2
Device(config-policy-tag)# end
```
request platform software trace archive

To archive all the trace logs relevant to all the processes running on a system since the last reload on the switches and to save this in the specified location, use the **request platform software trace archive** command in privileged EXEC or user EXEC mode.

```
request platform software trace archive [last number-of-days [days [target location] ]] | target location
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>last number-of-days</td>
<td>Specifies the number of days for which the trace files have to be archived.</td>
</tr>
<tr>
<td>target location</td>
<td>Specifies the location and name of the archive file.</td>
</tr>
</tbody>
</table>

**Command Modes**

- User EXEC (>
- Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Denali 16.1.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This archive file can be copied from the system, using the tftp or scp commands.

**Examples**

This example shows how to archive all the trace logs of the processes running on the switch since the last 5 days:

```
Device# request platform software trace archive last 5 days target flash:test_archive
```
rf tag

To configure an RF tag to the AP, use the `rf tag` command.

```
rf tag rf-tag-name
```

**Syntax Description**

- `rf-tag-name` RF tag name.

**Command Default**

None

**Command Modes**

config-ap-tag

**Command History**

<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>

**Usage Guidelines**

The AP will disconnect and rejoin after running this command.

**Example**

The following example shows how to configure an RF tag:

```
Device(config-ap-tag)# rf-tag rftag1
```
rrc-evaluation

To configure Resource Reservation Control (RRC) reevaluation admission, use the **rrc-evaluation** command.

```
rrc-evaluation {initial | periodic}
```

**Syntax Description**

- **initial** Configures initial admission evaluation.
- **periodic** Configures periodic admission evaluation.

**Command Default**

None

**Command Modes**

config-media-stream

**Command History**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure the RRC reevaluation admission to initial admission evaluation.

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless media-stream group my-media-group 224.0.0.0 224.0.0.223
Device(config-media-stream)# rrc-evaluation initial
```
security

To configure mesh security, use the `security` command.

```
security { eap | psk }
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>eap</td>
<td>Configure mesh security EAP for Mesh AP.</td>
</tr>
<tr>
<td>psk</td>
<td>Configure mesh security PSK for Mesh AP</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th>EAP</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Command Modes</th>
<th>config-wireless-mesh-profile</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<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>

**Examples**

The following example shows how to configure mesh security with EAP protocol on an Mesh AP:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless profile mesh profile-name
Device(config-wireless-mesh-profile)# security eap
```
security dot1x authentication-list

To configure security authentication list for IEEE 802.1x, use the `security dot1x authentication-list auth-list-name` command.

```
security dot1x authentication-list auth-list-name
```

### Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>auth-list-name</code></td>
<td>Authentication list name.</td>
</tr>
</tbody>
</table>

### Command Default

None

### Command Modes

config-wlan

### 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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to configure security authentication list for IEEE 802.1x:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan-name
Device(config-wlan)# security dot1x authentication-list auth-list-realm
```
**security ft**

To configure 802.11r fast transition parameters, use the `security ft` command. To configure fast transition over the air, use the `no security ft over-the-ds` command.

```
security ft [{over-the-ds|reassociation-timeout timeout-in-seconds}]
no security ft [{over-the-ds|reassociation-timeout}]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>over-the-ds</code></td>
<td>(Optional) Specifies that the 802.11r fast transition occurs over a distributed system. The no form of the command with this parameter configures security ft over the air.</td>
</tr>
<tr>
<td><code>reassociation-timeout</code></td>
<td>(Optional) Configures the reassociation timeout interval.</td>
</tr>
<tr>
<td><code>timeout-in-seconds</code></td>
<td>(Optional) Specifies the reassociation timeout interval in seconds. The valid range is between 1 to 100. The default value is 20.</td>
</tr>
</tbody>
</table>

**Command Default**
The feature is disabled.

**Command Modes**
WLAN configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.3SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
None

WLAN Security must be enabled.

**Example**
The following example configures security FT configuration for an open WLAN:

```
Device# wlan test
Device(config-wlan)# client vlan 0140
Device(config-wlan)# no mobility anchor sticky
Device(config-wlan)# no security wpa
Device(config-wlan)# no security wpa2 akm dot1x
Device(config-wlan)# no security wpa wpa2
Device(config-wlan)# no security wpa wpa2 ciphers aes
Device(config-wlan)# security ft
Device(config-wlan)# shutdown
```

The following example shows a sample security FT on a WPA-enabled WLAN:

```
Device# wlan test
Device(config-wlan)# client vlan 0140
Device(config-wlan)# no security wpa akm dot1x
Device(config-wlan)# security wpa akm ft psk
Device(config-wlan)# security wpa akm psk set-key ascii 0 test-test
```
Device(config-wlan)# security ft
Device(config-wlan)# no shutdown
security level (IPv6 snooping)

To specify the level of security enforced, use the security-level command in IPv6 snooping policy configuration mode.

```
security_level {glean | guard | inspect}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glean</td>
<td>Extracts addresses from the messages and installs them into the binding table without performing any verification.</td>
</tr>
<tr>
<td>guard</td>
<td>Performs both glean and inspect. Additionally, RA and DHCP server messages are rejected unless they are received on a trusted port or another policy authorizes them.</td>
</tr>
<tr>
<td>inspect</td>
<td>Validates messages for consistency and conformance; in particular, address ownership is enforced. Invalid messages are dropped.</td>
</tr>
</tbody>
</table>

**Command Default**

The default security level is guard.

**Command Modes**

IPv6 snooping configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

This example shows how to define an IPv6 snooping policy name as policy1, place the device in IPv6 snooping configuration mode, and configure the security level as inspect:

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# security-level inspect
```
**security pmf**

To configure 802.11w Management Frame Protection (PMF) on a WLAN, use the `security pmf` command. To disable management frame protection, use the `no` form of the command.

```
security pmf {association-comeback
association-comeback-time-seconds|mandatory|optional|saquery-retry-time saquery-retry-time-milliseconds}
no security pmf [{association-comeback
association-comeback-time-seconds|mandatory|optional|saquery-retry-time
saquery-retry-time-milliseconds}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>association-comeback</td>
<td>Configures the 802.11w association comeback time.</td>
</tr>
<tr>
<td>association-comeback-time-seconds</td>
<td>Association comeback interval in seconds. Time interval that an associated client must wait before the association is tried again after it is denied with a status code 30. The status code 30 message is &quot;Association request rejected temporarily; Try again later.&quot; The range is from 1 through 20 seconds.</td>
</tr>
<tr>
<td>mandatory</td>
<td>Specifies that clients are required to negotiate 802.11w PMF protection on the WLAN.</td>
</tr>
<tr>
<td>optional</td>
<td>Specifies that the WLAN does not mandate 802.11w support on clients. Clients with no 802.11w capability can also join.</td>
</tr>
<tr>
<td>saquery-retry-time</td>
<td>Time interval identified before which the SA query response is expected. If the device does not get a response, another SA query is tried.</td>
</tr>
<tr>
<td>saquery-retry-time-milliseconds</td>
<td>The saquery retry time in milliseconds. The range is from 100 to 500 ms. The value must be specified in multiples of 100 milliseconds.</td>
</tr>
</tbody>
</table>

**Command Default**

PMF is disabled.

**Command Modes**

WLAN configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.3SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You must have WPA (Wi-Fi Protected Access) and AKM (Authentication Key Management) configured to use this feature. See Related Command section for more information on configuring the security parameters.

802.11w introduces an Integrity Group Temporal Key (IGTK) that is used to protect broadcast or multicast robust management frames. IGTK is a random value, assigned by the authenticator station (device) used to protect MAC management protocol data units (MMPDUs) from the source STA. The 802.11w IGTK key is
derived using the four-way handshake and is used only on WLANs that are configured with WPA2 security at Layer 2.

This example shows how to enable the association comeback value at 15 seconds.

```
Device(config-wlan)# security pmf association-comeback 15
```

This example shows how to configure mandatory 802.11w MPF protection for clients on a WLAN:

```
Device(config-wlan)# security pmf mandatory
```

This example shows how to configure optional 802.11w MPF protection for clients on a WLAN:

```
Device(config-wlan)# security pmf optional
```

This example shows how to configure the saquery parameter:

```
Device(config-wlan)# security pmf saquery-retry-time 100
```

This example shows how to disable the PMF feature:

```
Device(config-wlan)# no security pmf
```
security static-wep-key

To configure static WEP keys on a WLAN, use the security static-wep-key command.

```
security static-wep-key {authentication {open | sharedkey} | encryption {104 | 40} {ascii | hex | {0 | 8}} wep-key | wep-index }
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>open</td>
<td>Open system authentication.</td>
</tr>
<tr>
<td>sharedkey</td>
<td>Shared key authentication.</td>
</tr>
<tr>
<td>0</td>
<td>Specifies an UNENCRYPTED password is used.</td>
</tr>
<tr>
<td>8</td>
<td>Specifies an AES encrypted password is used.</td>
</tr>
<tr>
<td>wep-key</td>
<td>Enter the name of the WEP key.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

config-wlan

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to authenticate 802.11 using shared key:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan profile-name wlan-id
Device(config-wlan)# security static-wep-key authentication sharedkey
```
security web-auth

To change the status of web authentication used on a WLAN, use the `security web-auth` command. To disable web authentication on a WLAN, use the `no` form of the command.

```
security web-auth [{authentication-list authentication-list-name|on-macfilter-failure|parameter-map parameter-map-name}]  
no security web-auth [{authentication-list [authentication-list-name]|on-macfilter-failure|parameter-map [parameter-map-name]}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>authentication-list</code></td>
<td>Sets the authentication list for IEEE 802.1x.</td>
</tr>
<tr>
<td><code>authentication-list-name</code></td>
<td></td>
</tr>
<tr>
<td><code>on-macfilter-failure</code></td>
<td>Enables web authentication on MAC failure.</td>
</tr>
<tr>
<td><code>parameter-map</code></td>
<td>Configures the parameter map.</td>
</tr>
<tr>
<td><code>parameter-map-name</code></td>
<td></td>
</tr>
</tbody>
</table>

**Command Default**

Web authentication is disabled.

**Command Modes**

WLAN configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure the authentication-list web authentication on a WLAN:

```
Device(config-wlan)# security web-auth authentication-list test
```
To configure authentication key management using Cisco Centralized Key Management (CCKM), use the `security wpa akm` command. To disable the authentication key management for Cisco Centralized Key Management, use the `no` form of the command.

```
security wpa [{\}akm {cckm|dot1x|ft|pmf|psk} \{wpa1 \{ciphers {aes|tkip}\} | wpa2 \{ciphers {aes|tikp}\}]}]
no security wpa [{\}akm {cckm|dot1x|ft|pmf|psk} \{wpa1 \{ciphers {aes|tkip}\} | wpa2 \{ciphers {aes|tikp}\}]}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>akm</code></td>
<td>Configures the Authentication Key Management (AKM) parameters.</td>
</tr>
<tr>
<td><code>aes</code></td>
<td>Configures AES (Advanced Encryption Standard) encryption support.</td>
</tr>
<tr>
<td><code>cckm</code></td>
<td>Configures Cisco Centralized Key Management support.</td>
</tr>
<tr>
<td><code>ciphers</code></td>
<td>Configures WPA ciphers.</td>
</tr>
<tr>
<td><code>dot1x</code></td>
<td>Configures 802.1x support.</td>
</tr>
<tr>
<td><code>ft</code></td>
<td>Configures fast transition using 802.11r.</td>
</tr>
<tr>
<td><code>pmf</code></td>
<td>Configures 802.11w management frame protection.</td>
</tr>
<tr>
<td><code>psk</code></td>
<td>Configures 802.11r fast transition pre-shared key (PSK) support.</td>
</tr>
<tr>
<td><code>tkip</code></td>
<td>Configures Temporal Key Integrity Protocol (TKIP) encryption support.</td>
</tr>
<tr>
<td><code>wpa2</code></td>
<td>Configures Wi-Fi Protected Access 2 (WPA2) support.</td>
</tr>
</tbody>
</table>

**Command Default**

By default Wi-Fi Protected Access 2, 802.1x are enabled. WPA2, PSK, CCKM, FT dot1x, FT PSK, PMF dot1x, PMF PSK, FT Support are disabled. The FT Reassociation timeout is set to 20 seconds, PMF SA Query time is set to 200.

**Command Modes**

WLAN configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.3SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
Example

The following example shows how to configure CCKM on the WLAN.

```
Device(config-wlan)#security wpa akm cckm
```
service-policy (Wired)

To apply a policy map to a physical port or a switch virtual interface (SVI), use the `service-policy` command in interface configuration mode. Use the `no` form of this command to remove the policy map and port association.

```
service-policy {input | output} policy-map-name
no service-policy {input | output} policy-map-name
```

### Syntax Description

- **input policy-map-name**: Apply the specified policy map to the input of a physical port or an SVI.
- **output policy-map-name**: Apply the specified policy map to the output of a physical port or an SVI.

### Command Default

No policy maps are attached to the port.

### Command Modes

WLAN interface configuration

### Command History

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

### Usage Guidelines

A policy map is defined by the `policy map` command.

Only one policy map is supported per port, per direction. In other words, only one input policy and one output policy is allowed on any one port.

You can apply a policy map to incoming traffic on a physical port or on an SVI. *QoS Configuration Guide (Catalyst 3850 Switches)*.

### Note

Though visible in the command-line help strings, the `history` keyword is not supported, and you should ignore the statistics that it gathers.

### Examples

This example shows how to apply `plcmap1` to an physical ingress port:

```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# service-policy input plcmap1
```

This example shows how to remove `plcmap2` from a physical port:

```
Device(config)# interface gigabitethernet2/0/2
Device(config-if)# no service-policy input plcmap2
```

The following example displays a VLAN policer configuration. At the end of this configuration, the VLAN policy map is applied to an interface for QoS:

```
Device# configure terminal
```
Device(config)# class-map vlan100
Device(config-cmap)# match vlan 100
Device(config-cmap)# exit
Device(config)# policy-map vlan100
Device(config-pmap)# policy-map class vlan100
Device(config-pmap-c)# police 100000 bc conform-action transmit exceed-action drop
Device(config-pmap-c-police)# end
Device# configure terminal
Device(config)# interface gigabitEthernet1/0/5
Device(config-if)# service-policy input vlan100

You can verify your settings by entering the **show running-config** privileged EXEC command.
service-policy (WLAN)

To configure the WLAN quality of service (QoS) service policy, use the `service-policy` command. To disable a QoS policy on a WLAN, use the `no` form of this command.

```
service-policy [client] {input|output} policy-name
no service-policy [client] {input|output} policy-name
```

**Syntax Description**

- `client` (Optional) Assigns a policy map to all clients in the WLAN.
- `input` Assigns an input policy map.
- `output` Assigns an output policy map.
- `policy-name` The policy name.

**Command Default**

No policies are assigned and the state assigned to the policy is None.

**Command Modes**

WLAN configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Examples**

This example shows how to configure the input QoS service policy on a WLAN:

```text
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# service-policy input policy-test
```

This example shows how to disable the input QoS service policy on a WLAN:

```text
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no service-policy input policy-test
```

This example shows how to configure the output QoS service policy on a WLAN to platinum (precious metal policy):

```text
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# service-policy output platinum
```
service-policy qos

To configure a QoS service policy, use the `service-policy qos` command.

```
service-policy qos {input|output} policy-name
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>input</td>
<td>Input QoS policy.</td>
</tr>
<tr>
<td>output</td>
<td>Output QoS policy.</td>
</tr>
<tr>
<td>policy-name</td>
<td>Policy name.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

config-service-template

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure an output QoS policy:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# service-template fabric-profile-name
Device(config-service-template)# service-policy qos output policy-name
```
service-template

To configure service template, use the `service-template` command.

```plaintext
service-template service-template-name { access-group acl_list | vlan vlan_id | absolute-timer seconds | service-policy qos { input | output } }
```

**Syntax Description**

- **service-template-name**: Name of the service template.
- **acl_list**: Access list name to be applied.
- **vlan_id**: VLAN ID. The VLAN ID value ranges from 1 to 4094.
- **seconds**: Session timeout value for service template. The session timeout value ranges from 1 to 65535 seconds.
- **service-policy qos { input | output }**: QoS policies for client.

**Command Default**

None

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3E</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

None

The following example shows how to configure service template:

```plaintext
Device#configure terminal
Device(config)#service-template cisco-phone-template
Device(config-service-template)#access-group foo-acl
Device(config-service-template)#vlan 100
Device(config-service-template)#service-policy qos input foo-qos
Device(config-service-template)#end
```
To configure session timeout for clients associated to a WLAN, use the `session-timeout` command. To disable a session timeout for clients that are associated to a WLAN, use the `no` form of this command.

```
session-timeout seconds
no session-timeout
```

**Syntax Description**

- `seconds` Timeout or session duration in seconds. A value of zero (0) is equivalent to no timeout. The range is from 300 to 86400.

**Command Default**

The client timeout is set to 1800 seconds for WLANs that are configured with dot1x security. The client timeout is set to 0 for open WLANs.

**Command Modes**

WLAN configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

This example shows how to configure a session timeout to 300 seconds:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# session-timeout 300
```

This example shows how to disable a session timeout:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no session-timeout
```
To classify IP traffic by setting a Differentiated Services Code Point (DSCP) or an IP-precedence value in the packet, use the `set` command in policy-map class configuration mode. Use the `no` form of this command to remove traffic classification.

```
set
cos|dscp|precedence|ip|qos-group|wlan
set cos
{cos-value} | {cos|dscp|precedence|qos-group|wlan} [{table table-map-name}]
set dscp
{dscp-value} | {cos|dscp|precedence|qos-group|wlan} [{table table-map-name}]
set ip {dscp|precedence}
set precedence {precedence-value} | {cos|dscp|precedence|qos-group} [{table table-map-name}]
set qos-group
{qos-group-value|dscp [{table table-map-name}]} {precedence [{table table-map-name}]}]
set wlan user-priority
user-priority-value|costable {table-map-name} | dscp|table-map-name|qos-group|table-map-name|wlantable {table-map-name}
```
Syntax Description

cos

Sets the Layer 2 class of service (CoS) value or user priority of an outgoing packet. You can specify these values:

- **cos-value**—CoS value from 0 to 7. You also can enter a mnemonic name for a commonly used value.

- Specify a packet-marking category to set the CoS value of the packet. If you also configure a table map for mapping and converting packet-marking values, this establishes the "map from" packet-marking category. Packet-marking category keywords:
  
  - **cos**—Sets a value from the CoS value or user priority.
  
  - **dscp**—Sets a value from packet differentiated services code point (DSCP).
  
  - **precedence**—Sets a value from packet precedence.
  
  - **qos-group**—Sets a value from the QoS group.
  
  - **wlan**—Sets the WLAN user priority values.

  - (Optional) **table  table-map-name**—Indicates that the values set in a specified table map are used to set the CoS value. Enter the name of the table map used to specify the CoS value. The table map name can be a maximum of 64 alphanumeric characters.

  If you specify a packet-marking category but do not specify the table map, the default action is to copy the value associated with the packet-marking category as the CoS value. For example, if you enter the **set cos precedence** command, the precedence (packet-marking category) value is copied and used as the CoS value.
### dscp

Sets the differentiated services code point (DSCP) value to mark IP(v4) and IPv6 packets. You can specify these values:

- **cos-value**—Number that sets the DSCP value. The range is from 0 to 63. You also can enter a mnemonic name for a commonly used value.

- Specify a packet-marking category to set the DSCP value of the packet. If you also configure a table map for mapping and converting packet-marking values, this establishes the "map from" packet-marking category. Packet-marking category keywords:
  - **cos**—Sets a value from the CoS value or user priority.
  - **dscp**—Sets a value from packet differentiated services code point (DSCP).
  - **precedence**—Sets a value from packet precedence.
  - **qos-group**—Sets a value from the QoS group.
  - **wlan**—Sets a value from WLAN.

- **table table-map-name**—Indicates that the values set in a specified table map will be used to set the DSCP value. Enter the name of the table map used to specify the DSCP value. The table map name can be a maximum of 64 alphanumeric characters.

If you specify a packet-marking category but do not specify the table map, the default action is to copy the value associated with the packet-marking category as the DSCP value. For example, if you enter the set dscp cos command, the CoS value (packet-marking category) is copied and used as the DSCP value.

### ip

Sets IP values to the classified traffic. You can specify these values:

- **dscp**—Specify an IP DSCP value from 0 to 63 or a packet marking category.

- **precedence**—Specify a precedence-bit value in the IP header; valid values are from 0 to 7 or specify a packet marking category.
**precedence**

Sets the precedence value in the packet header. You can specify these values:

- **precedence-value** — Sets the precedence bit in the packet header; valid values are from 0 to 7. You also can enter a mnemonic name for a commonly used value.

- Specify a packet marking category to set the precedence value of the packet.
  - **cos**—Sets a value from the CoS or user priority.
  - **dscp**—Sets a value from packet differentiated services code point (DSCP).
  - **precedence**—Sets a value from packet precedence.
  - **qos-group**—Sets a value from the QoS group.

- (Optional) **table table-map-name**—Indicates that the values set in a specified table map will be used to set the precedence value. Enter the name of the table map used to specify the precedence value. The table map name can be a maximum of 64 alphanumeric characters.

  If you specify a packet-marking category but do not specify the table map, the default action is to copy the value associated with the packet-marking category as the precedence value. For example, if you enter the `set precedence cos` command, the CoS value (packet-marking category) is copied and used as the precedence value.
**qos-group**

Assigns a QoS group identifier that can be used later to classify packets.

- **qos-group-value**—Sets a QoS value to the classified traffic. The range is 0 to 31. You also can enter a mnemonic name for a commonly used value.

- **dscp**—Sets the original DSCP field value of the packet as the QoS group value.

- **precedence**—Sets the original precedence field value of the packet as the QoS group value.

- *(Optional)* **table table-map-name**—Indicates that the values set in a specified table map will be used to set the DSCP or precedence value. Enter the name of the table map used to specify the value. The table map name can be a maximum of 64 alphanumeric characters.

If you specify a packet-marking category (*dscp* or *precedence*) but do not specify the table map, the default action is to copy the value associated with the packet-marking category as the QoS group value. For example, if you enter the `set qos-group precedence` command, the precedence value (packet-marking category) is copied and used as the QoS group value.
**wlan user-priority wlan-user-priority**

Assigns a WLAN user-priority to the classified traffic. You can specify these values:

- **wlan-user-priority**—Sets a WLAN user priority to the classified traffic. The range is 0 to 7.
- **cos**—Sets the Layer 2 CoS field value as the WLAN user priority.
- **dscp**—Sets the DSCP field value as the WLAN user priority.
- **precedence**—Sets the precedence field value as the WLAN user priority.
- **wlan**—Sets the WLAN user priority field value as the WLAN user priority.
- **(Optional)** table table-map-name—Indicates that the values set in a specified table map will be used to set the WLAN user priority value. Enter the name of the table map used to specify the value. The table map name can be a maximum of 64 alphanumeric characters.

If you specify a packet-marking category but do not specify the table map, the default action is to copy the value associated with the packet-marking category as the WLAN user priority. For example, if you enter the **set wlan user-priority cos** command, the cos value (packet-marking category) is copied and used as the WLAN user priority.

---

**Command Default**

No traffic classification is defined.

**Command Modes**

Policy-map class configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE 3.3SE</td>
<td>The cos, dscp, qos-group, wlan table table-map-name, keywords were added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

When you configure the **set dscp cos** command, note the following: The CoS value is a 3-bit field, and the DSCP value is a 6-bit field. Only the three bits of the CoS field are used.
When you configure the `set dscp qos-group` command, note the following:

- The valid range for the DSCP value is a number from 0 to 63. The valid value range for the QoS group is a number from 0 to 99.
- If a QoS group value falls within both value ranges (for example, 44), the packet-marking value is copied and the packets is marked.
- If QoS group value exceeds the DSCP range (for example, 77), the packet-marking value is not be copied and the packet is not marked. No action is taken.

The `set qos-group` command cannot be applied until you create a service policy in policy-map configuration mode and then attach the service policy to an interface or ATM virtual circuit (VC).

To return to policy-map configuration mode, use the `exit` command. To return to privileged EXEC mode, use the `end` command.

### Examples

This example shows how to assign DSCP 10 to all FTP traffic without any policers:

```
Device(config)# policy-map policy_ftp
Device(config-pmap)# class-map ftp_class
Device(config-cmap)# exit
Device(config)# policy policy_ftp
Device(config-pmap)# class ftp_class
Device(config-pmap-c)# set dscp 10
Device(config-pmap)# exit
```

You can verify your settings by entering the `show policy-map` privileged EXEC command.
**set trace capwap ap ha**

To trace the control and provisioning of wireless access point high availability, use the `set trace capwap ap ha` command.

```
set trace capwap ap ha [\{detail\|event\|dump \}|\{filter \]|\{none [switch switch]\}filter_name [filter_value [switch switch]\}]\{filtered\}switch\level \{default\trace_level\} [switch switch]\}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>detail</code></td>
<td>(Optional) Specifies the wireless CAPWAP HA details.</td>
</tr>
<tr>
<td><code>event</code></td>
<td>(Optional) Specifies the wireless CAPWAP HA events.</td>
</tr>
<tr>
<td><code>dump</code></td>
<td>(Optional) Specifies the wireless CAPWAP HA output.</td>
</tr>
<tr>
<td><code>filter mac</code></td>
<td>Specifies the MAC address.</td>
</tr>
<tr>
<td><code>switch switch number</code></td>
<td>Specifies the switch number.</td>
</tr>
<tr>
<td><code>none</code></td>
<td>(Optional) Specifies the no filter option.</td>
</tr>
<tr>
<td><code>switch switch</code></td>
<td>(Optional) Specifies the device number.</td>
</tr>
<tr>
<td><code>filter name</code></td>
<td>Trace adapted flag filter name.</td>
</tr>
<tr>
<td><code>filter_value</code></td>
<td>(Optional) Value of the filter.</td>
</tr>
<tr>
<td><code>switch switch</code></td>
<td>(Optional) Specifies the device number.</td>
</tr>
<tr>
<td><code>filtered</code></td>
<td>Specifies the filtered traces messages.</td>
</tr>
<tr>
<td><code>switch switch</code></td>
<td>Specifies the switch number.</td>
</tr>
<tr>
<td><code>level</code></td>
<td>Specifies the trace level.</td>
</tr>
<tr>
<td><code>default</code></td>
<td>Specifies the unset trace level value.</td>
</tr>
<tr>
<td><code>trace_level</code></td>
<td>Specifies the trace level.</td>
</tr>
<tr>
<td><code>switch switch</code></td>
<td>(Optional) Specifies the device number.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

This example shows how to display the wireless CAPWAP HA:

```
Device# set trace capwap ap ha detail filter mac WORD switch number
```
set trace mobility ha

To debug the wireless mobility high availability, use the `set trace mobility ha` command.

```
set trace mobility ha [{event|detail|dump}] {filter[mac WORD switch switch number] [{none [switch switch]filter_name filter_value [switch switch]}]} level {default|trace_level} [switch switch] {filtered|switch}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>event</td>
<td>(Optional) Specifies the wireless mobility high availability events.</td>
</tr>
<tr>
<td>detail</td>
<td>(Optional) Specifies the wireless mobility high availability details.</td>
</tr>
<tr>
<td>dump</td>
<td>(Optional) Specifies the wireless mobility high availability output.</td>
</tr>
<tr>
<td>filter</td>
<td>Specifies to trace adapted flag filter.</td>
</tr>
<tr>
<td>mac</td>
<td>Specifies the MAC address.</td>
</tr>
<tr>
<td>WORD switch</td>
<td>Specifies the switch.</td>
</tr>
<tr>
<td>switch number</td>
<td>Specifies the switch number. The value ranges from one to four.</td>
</tr>
<tr>
<td>none</td>
<td>Specifies no trace adapted flag filter.</td>
</tr>
<tr>
<td>switch switch</td>
<td>(Optional) Specifies the device number.</td>
</tr>
<tr>
<td>filter_name</td>
<td>Trace adapted flag filter name.</td>
</tr>
<tr>
<td>filter_value</td>
<td>Trace adapted flag filter value.</td>
</tr>
<tr>
<td>switch switch</td>
<td>Specifies the device number.</td>
</tr>
<tr>
<td>level</td>
<td>Specifies the trace level value.</td>
</tr>
<tr>
<td>default</td>
<td>Specifies the un-set trace level value.</td>
</tr>
<tr>
<td>trace_level</td>
<td>Specifies the trace level value.</td>
</tr>
<tr>
<td>switch switch</td>
<td>Specifies the device number.</td>
</tr>
<tr>
<td>filtered</td>
<td>Specifies the filtered trace messages.</td>
</tr>
<tr>
<td>switch</td>
<td>Specifies the switch.</td>
</tr>
</tbody>
</table>
This example shows how to display wireless mobility high availability details:

```
Device# set trace mobility ha detail filter mac WORD
[08/27/13 10:38:35.349 UTC 1 8135] Invalid src ip: 169.254.1.1
[08/27/13 10:38:54.393 UTC 3 8135] Mobility version mismatch, v10 received, or msglen mismatch msglen=74 recvBytes=0, dropping
```
set trace qos ap ha

To trace wireless Quality of Service (QoS) high availability, use the `set trace qos ap ha` command.

```
set trace QOS ap ha [{event|error}] [filter [{MACnone [switch switch]}]filter_name [filter_value [switch switch]]]level {default trace_level} [switch switch]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>event</code></td>
<td>(Optional) Specifies trace QoS wireless AP event.</td>
</tr>
<tr>
<td><code>event mac</code></td>
<td>Specifies the MAC address of the AP.</td>
</tr>
<tr>
<td><code>event none</code></td>
<td>Specifies no MAC address value.</td>
</tr>
<tr>
<td><code>error</code></td>
<td>(Optional) Specifies trace QoS wireless AP errors.</td>
</tr>
<tr>
<td><code>error mac</code></td>
<td>Specifies the MAC address of the AP.</td>
</tr>
<tr>
<td><code>error none</code></td>
<td>Specifies no value.</td>
</tr>
<tr>
<td><code>filter</code></td>
<td>Specifies the trace adapted flag filter.</td>
</tr>
<tr>
<td><code>filter mac</code></td>
<td>Specifies the MAC address of the AP.</td>
</tr>
<tr>
<td><code>filter none</code></td>
<td>Specifies no value.</td>
</tr>
<tr>
<td><code>switch switch</code></td>
<td>Specifies the switch number.</td>
</tr>
<tr>
<td><code>filter_name</code></td>
<td>(Optional) Specifies the switch filter name.</td>
</tr>
<tr>
<td><code>filter_value</code></td>
<td>(Optional) Specifies the switch filter value. Value is one.</td>
</tr>
<tr>
<td><code>switch switch</code></td>
<td>(Optional) Specifies the switch number. Value is one.</td>
</tr>
<tr>
<td><code>level</code></td>
<td>Specifies the trace level.</td>
</tr>
<tr>
<td><code>default</code></td>
<td>Specifies the trace QoS wireless AP default.</td>
</tr>
<tr>
<td><code>trace_level</code></td>
<td>Trace level.</td>
</tr>
<tr>
<td><code>switch switch</code></td>
<td>(Optional) Specifies the switch number. Value is one.</td>
</tr>
</tbody>
</table>

### Command Default

None

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

This example shows how to trace wireless QoS high availability:

```
Device# set trace QOS ap ha
```
To SGT tag for a fabric profile, use the `sgt-tag` command.

```
sgt-tag value
```

**Syntax Description**

```
value  SGT tag value. Valid range is 2 to 65519.
```

**Command Default**

The default SGT tag value is 0.

**Command Modes**

config-wireless-fabric

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure an SGT tag value:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless profile fabric fabric-profile-name
Device(config-wireless-fabric)# sgt tag 8
```
shutdown

To shut down VLAN switching, use the `shutdown` command in global configuration mode. To disable the configuration set, use the `no` form of this command.

```
shutdown [ vlan vlan-id ]
no shutdown
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vlan vlan-id</code></td>
<td>VLAN ID of VLAN to shutdown.</td>
</tr>
</tbody>
</table>

### Command Default

No default behavior or values.

### Command Modes

Global configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOSXE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

This example shows how to shutdown a VLAN:

```
Device(config)# vlan open1
Device(config-wlan)# shutdown
```

This example shows that the access point is not shut down:

```
Device# configure terminal
Device(config)# ap name 3602a no shutdown
```
site-tag

To map a site tag to the AP, use the `site-tag` command.

```
site-tag site-tag-name
```

**Syntax Description**

<table>
<thead>
<tr>
<th>site-tag-name</th>
<th>Name of the site tag.</th>
</tr>
</thead>
</table>

**Command Default**

None

**Command Modes**

config-ap-tag

**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>

**Usage Guidelines**

The AP will disconnect and rejoin after running this command.

**Example**

The following example shows how to configure a site tag:

```
Device(config-ap-tag)# site-tag sitetag1
```
static-ip-mobility

To configure static IP mobility, use the static-ip-mobility command in wireless-policy configuration mode. To disable the configuration, use the no form of this command.

static-ip-mobility

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

wireless-policy configuration mode

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>

Example

This example shows how to enable static IP mobility:

Device# configure terminal
Device(config)# wireless profile policy test-policy
Device(config-wireless-policy)# static-ip-mobility
**switchport**

To put an interface that is in Layer 3 mode into Layer 2 mode for Layer 2 configuration, use the `switchport` command in interface configuration mode. To put an interface in Layer 3 mode, use the `no` form of this command.

```
switchport
no  switchport
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

By default, all interfaces are in Layer 2 mode.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `no switchport` command (without parameters) to set the interface to the routed-interface status and to erase all Layer 2 configurations. You must use this command before assigning an IP address to a routed port.

**Note**

This command is not supported on devices running the LAN Base feature set.

Entering the `no switchport` command shuts the port down and then reenables it, which might generate messages on the device to which the port is connected.

When you put an interface that is in Layer 2 mode into Layer 3 mode (or the reverse), the previous configuration information related to the affected interface might be lost, and the interface is returned to its default configuration.

**Note**

If an interface is configured as a Layer 3 interface, you must first enter the `switchport` command to configure the interface as a Layer 2 port. Then you can enter the `switchport access vlan` and `switchport mode` commands.

The `switchport` command is not used on platforms that do not support Cisco-routed ports. All physical ports on such platforms are assumed to be Layer 2-switched interfaces.

You can verify the port status of an interface by entering the `show running-config` privileged EXEC command.

**Examples**

This example shows how to cause an interface to cease operating as a Layer 2 port and become a Cisco-routed port:

```
Device(config-if)# no switchport
```
This example shows how to cause the port interface to cease operating as a Cisco-routed port and convert to a Layer 2 switched interface:

```
Device(config-if)# switchport
```
**switchport access vlan**

To configure a port as a static-access port, use the `switchport access vlan` command in interface configuration mode. To reset the access mode to the default VLAN mode for the device, use the `no` form of this command.

```bash
switchport access vlan {vlan-id | name vlan_name}
no switchport access vlan
```

**Syntax Description**

- **vlan-id**: VLAN ID of the access mode VLAN; the range is 1 to 4094.

**Command Default**

The default access VLAN and trunk interface native VLAN is a default VLAN corresponding to the platform or interface hardware.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Denali 16.2.1</td>
<td>The <code>name vlan_name</code> keyword was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The port must be in access mode before the `switchport access vlan` command can take effect.
- If the switchport mode is set to `access vlan vlan-id`, the port operates as a member of the specified VLAN. An access port can be assigned to only one VLAN.
- The `no switchport access` command resets the access mode VLAN to the appropriate default VLAN for the device.

**Examples**

This example shows how to change a switched port interface that is operating in access mode to operate in VLAN 2 instead of the default VLAN:

```bash
Device(config-if)# switchport access vlan 2
```

This example show how to first populate the VLAN database by associating a VLAN ID with a VLAN name, and then configure the VLAN (using the name) on an interface, in the access mode:

You can also verify your configuration by entering the `show interfaces interface-id switchport` in privileged EXEC command and examining information in the Access Mode VLAN: row.

**Part 1 - Making the entry in the VLAN database:**

```bash
Device# configure terminal
Device(config)# vlan 33
Device(config-vlan)# name test
Device(config-vlan)# end
Device#
```

**Part 2 - Checking the VLAN database**

```bash
Device # show vlan id 33
VLAN  Name      Status  Ports
-------  ---------  ------
```

---

465
### Part 3 - Assigning VLAN to the interface by using the name of the VLAN

```
Device # configure terminal
Device(config)# interface GigabitEthernet3/1/1
Device(config-if)# switchport mode access
Device(config-if)# switchport access vlan name test
Device(config-if)#
```

### Part 4 - Verifying configuration

```
Device # show running-config interface GigabitEthernet3/1/1
Building configuration...
Current configuration : 113 bytes
!
interface GigabitEthernet3/1/1
  switchport access vlan 33
  switchport mode access
```

### Part 5 - Verifying interface switchport

```
Device # show interface GigabitEthernet3/1/1 switchport
Name: Gi3/1/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 33 (test)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: None
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```
switchport mode

To configure the VLAN membership mode of a port, use the `switchport mode` command in interface configuration mode. To reset the mode to the appropriate default for the device, use the `no` form of this command.

```
switchport mode {access|dynamic |{auto|desirable}|trunk}
noswitchport mode {access|dynamic |{auto|desirable}|trunk}
```

**Syntax Description**

- `access` Sets the port to access mode (either static-access or dynamic-access depending on the setting of the `switchport access vlan` interface configuration command). The port is set to access unconditionally and operates as a nontrunking, single VLAN interface that sends and receives nonencapsulated (non-tagged) frames. An access port can be assigned to only one VLAN.

- `dynamic auto` Sets the port trunking mode dynamic parameter to auto to specify that the interface convert the link to a trunk link. This is the default switchport mode.

- `dynamic desirable` Sets the port trunking mode dynamic parameter to desirable to specify that the interface actively attempt to convert the link to a trunk link.

- `trunk` Sets the port to trunk unconditionally. The port is a trunking VLAN Layer 2 interface. The port sends and receives encapsulated (tagged) frames that identify the VLAN of origination. A trunk is a point-to-point link between two devices or between a device and a router.

**Command Default**

The default mode is `dynamic auto`.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- **Note** Although visible in the CLI, the `dot1q-tunnel` keyword is not supported.

A configuration that uses the `access` or `trunk` keywords takes effect only when you configure the port in the appropriate mode by using the `switchport mode` command. The static-access and trunk configuration are saved, but only one configuration is active at a time.

When you enter `access` mode, the interface changes to permanent nontrunking mode and negotiates to convert the link into a nontrunk link even if the neighboring interface does not agree to the change.

When you enter `trunk` mode, the interface changes to permanent trunking mode and negotiates to convert the link into a trunk link even if the interface connecting to it does not agree to the change.
When you enter **dynamic auto** mode, the interface converts the link to a trunk link if the neighboring interface is set to **trunk** or **desirable** mode.

When you enter **dynamic desirable** mode, the interface becomes a trunk interface if the neighboring interface is set to **trunk**, **desirable**, or **auto** mode.

To autonegotiate trunking, the interfaces must be in the same VLAN Trunking Protocol (VTP) domain. Trunk negotiation is managed by the Dynamic Trunking Protocol (DTP), which is a point-to-point protocol. However, some internetworking devices might forward DTP frames improperly, which could cause misconfigurations. To avoid this problem, configure interfaces connected to devices that do not support DTP to not forward DTP frames, which turns off DTP.

- If you do not intend to trunk across those links, use the `switchport mode access` interface configuration command to disable trunking.
- To enable trunking to a device that does not support DTP, use the `switchport mode trunk` and `switchport nongotiate` interface configuration commands to cause the interface to become a trunk but to not generate DTP frames.

Access ports and trunk ports are mutually exclusive.

The IEEE 802.1x feature interacts with switchport modes in these ways:

- If you try to enable IEEE 802.1x on a trunk port, an error message appears, and IEEE 802.1x is not enabled. If you try to change the mode of an IEEE 802.1x-enabled port to trunk, the port mode is not changed.
- If you try to enable IEEE 802.1x on a port set to **dynamic auto** or **dynamic desirable**, an error message appears, and IEEE 802.1x is not enabled. If you try to change the mode of an IEEE 802.1x-enabled port to **dynamic auto** or **dynamic desirable**, the port mode is not changed.
- If you try to enable IEEE 802.1x on a dynamic-access (VLAN Query Protocol [VQP]) port, an error message appears, and IEEE 802.1x is not enabled. If you try to change an IEEE 802.1x-enabled port to dynamic VLAN assignment, an error message appears, and the VLAN configuration is not changed.

You can verify your settings by entering the `show interfaces interface-id switchport` privileged EXEC command and examining information in the **Administrative Mode** and **Operational Mode** rows.

### Examples

This example shows how to configure a port for access mode:

```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# switchport mode access
```

This example shows how set the port to dynamic desirable mode:

```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# switchport mode dynamic desirable
```

This example shows how to configure a port for trunk mode:

```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# switchport mode trunk
```
**tag rf**

To configure a policy tag for an AP filter, use the *tag rf* command.

```plaintext
tag rf  rf-tag
```

**Syntax Description**

<table>
<thead>
<tr>
<th>rftag</th>
<th>RF tag name.</th>
</tr>
</thead>
</table>

**Command Default**

None

**Command Modes**

config-ap-filter

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure a policy tag for an AP filter:

```plaintext
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# ap filter name ap-filter-name
Device(config-ap-filter)# rf tag rf-tag-name
```
To configure a site tag for an AP filter, use the `tag site site-tag` command.

```
tag site site-tag
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>site-tag</code></td>
<td>Name of the site tag.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

config-ap-filter

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure a site tag for an AP filter:

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

To configure the transport protocol for a flow exporter for, use the `transport` command in flow exporter configuration mode. To remove the transport protocol for a flow exporter, use the `no` form of this command.

```
transport udp udp-port
no transport udp udp-port
```

**Syntax Description**
- `udp udp-port`: Specifies User Datagram Protocol (UDP) as the transport protocol and the UDP port number.

**Command Default**
Flow exporters use UDP on port 9995.

**Command Modes**
Flow exporter configuration

**Command History**
- **Release** | **Modification**
  - Cisco IOS XE 3.2SE: This command was introduced.

**Usage Guidelines**
To return this command to its default settings, use the `no transport` or `default transport flow exporter` configuration command.

The following example configures UDP as the transport protocol and a UDP port number of 250:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# transport udp 250
```
trusted-port

To configure a port to become a trusted port, use the trusted-port command in IPv6 snooping policy mode or ND inspection policy configuration mode. To disable this function, use the no form of this command.

trusted-port
no trusted-port

Syntax Description
This command has no arguments or keywords.

Command Default
No ports are trusted.

Command Modes
ND inspection policy configuration
IPv6 snooping configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines
When the trusted-port command is enabled, limited or no verification is performed when messages are received on ports that have this policy. However, to protect against address spoofing, messages are analyzed so that the binding information that they carry can be used to maintain the binding table. Bindings discovered from these ports will be considered more trustworthy than bindings received from ports that are not configured to be trusted.

This example shows how to define an NDP policy name as policy1, place the switch in NDP inspection policy configuration mode, and configure the port to be trusted:

```
Device(config)# ipv6 nd inspection policy1
Device(config-nd-inspection)# trusted-port
```

This example shows how to define an IPv6 snooping policy name as policy1, place the switch in IPv6 snooping policy configuration mode, and configure the port to be trusted:

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# trusted-port
```
**type**

To display the contents of one or more files, use the `type` command in boot loader mode.

```
type filesystem:/file-url...
```

**Syntax Description**

- `filesystem`: Alias for a file system. Use `flash:` for the system board flash device; use `usbflash0:` for USB memory sticks.
- `/file-url...`: Path (directory) and name of the files to display. Separate each filename with a space.

**Command Default**

No default behavior or values.

**Command Modes**

Boot loader

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Filenames and directory names are case sensitive.

If you specify a list of files, the contents of each file appear sequentially.

**Examples**

This example shows how to display the contents of a file:

```plaintext
Device: type flash:image_file_name
version_suffix: universal-122-xx.SEx
version_directory: image_file_name
image_system_type_id: 0x00000002
image_name: image_file_name.bin
ios_image_file_size: 8919552
total_image_file_size: 11592192
image_feature: IP|LAYER_3|LIJS|MIN_DRAM_MEG=128
image_family: family
stacking_number: 1.34
board_ids: 0x00000068 0x00000069 0x0000006a 0x0000006b
info_end:
```
udp-timeout

To configure timeout value for UDP sessions, use the **udp-timeout** command.

```
udp-timeout  timeout_value
```

**Syntax Description**

- **timeout_value**: Is the timeout value for UDP sessions.
  
  The range is from 1 to 30 seconds.

  **Note**: The public-key and resolver parameter-map options are automatically populated with the default values. So, you need not change them.

**Command Default**

None

**Command Modes**

Profile configuration

**Command History**

<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>

**Example**

This example shows how to configure timeout value for UDP sessions:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# parameter-map type umbrella global
Device(config-profile)# token 57CC80106C087FB1B2A7BAB4F2F4373C00247166
Device(config-profile)# local-domain dns_wl
Device(config-profile)# udp-timeout 2
Device(config-profile)# end
```
To configure the Umbrella OpenDNS feature for WLAN, use the `umbrella-param-map` command.

**umbrella-param-map  umbrella-name**

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>umbrella-name</th>
</tr>
</thead>
</table>

**Command Default**

None

**Command Modes**

config-wireless-policy

**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>

**Example**

This example shows how to configure the Umbrella OpenDNS feature for WLAN:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless profile policy default-policy-profile
Device(config-wireless-policy)# umbrella-param-map global
Device(config-wireless-policy)# end
```
username

To add a user who can access the Cisco ISE-3315 using SSH, use the `username` command in configuration mode. If the user already exists, the password, the privilege level, or both change with this command. To delete the user from the system, use the `no` form of this command.

```plaintext
[no] username username password {hash | plain} password role {admin | user} [disabled [email email-address]] [email email-address]
```

For an existing user, use the following command option:

```plaintext
username username password role {admin | user} password
```

### Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>username</code></td>
<td>You should enter only one word which can include hyphen (-), underscore (_) and period (.). <strong>Note</strong> Only alphanumeric characters are allowed at an initial setup.</td>
</tr>
<tr>
<td><code>password</code></td>
<td>The command to use specify password and user role.</td>
</tr>
<tr>
<td><code>password</code></td>
<td>Password character length up to 40 alphanumeric characters. You must specify the password for all new users.</td>
</tr>
<tr>
<td>`hash</td>
<td>plain`</td>
</tr>
<tr>
<td>`role admin</td>
<td>user`</td>
</tr>
<tr>
<td><code>disabled</code></td>
<td>Disables the user according to the user’s email address.</td>
</tr>
<tr>
<td><code>email email-address</code></td>
<td>The user’s email address. For example, <a href="mailto:user1@example.com">user1@example.com</a>.</td>
</tr>
</tbody>
</table>

### Command Default

The initial user during setup.

### Command Modes

Configuration

### Usage Guidelines

The `username` command requires that the `username` and `password` keywords precede the `hash | plain` and the `admin | user` options.

### Example 1

```plaintext
ncs/admin(config)# username admin password hash ###### role admin
ncs/admin(config)#
```

### Example 2

```plaintext
ncs/admin(config)# username admin password plain Secr3tp@swd role admin
ncs/admin(config)#
```

### Example 3
ncs/admin(config)# username admin password plain Secr3tp@swd role admin email admin123@example.com
ncs/admin(config)#
To configure stream violation policy on periodic reevaluation, use the `violation` command.

```
violation {drop | fallback}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>drop</td>
<td>Stream will be dropped on periodic reevaluation.</td>
</tr>
<tr>
<td>fallback</td>
<td>Stream will be demoted to BestEffort class on periodic reevaluation.</td>
</tr>
</tbody>
</table>

### Command Default

None

### Command Modes

config-media-stream

### 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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to configure stream violation policy on periodic reevaluation:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless media-stream group my-media-group 224.0.0.0 224.0.0.223
Device(config-media-stream)# violation drop
```
To add a VLAN and to enter the VLAN configuration mode, use the `vlan` command in global configuration mode. To delete the VLAN, use the `no` form of this command.

```plaintext
vlan vlan-id  
no vlan vlan-id
```

**Syntax Description**  
- `vlan-id`  
  - ID of the VLAN to be added and configured. The range is 1 to 4094. You can enter a single VLAN ID, a series of VLAN IDs separated by commas, or a range of VLAN IDs separated by hyphens.

**Command Default**  
None

**Command Modes**  
Global configuration

**Command History**  
- **Release**  
  - Cisco IOS XE 3.2SE  
    - This command was introduced.

**Usage Guidelines**  
You can use the `vlan vlan-id` global configuration command to add normal-range VLANs (VLAN IDs 1 to 1005) or extended-range VLANs (VLAN IDs 1006 to 4094). Configuration information for normal-range VLANs is always saved in the VLAN database, and you can display this information by entering the `show vlan` privileged EXEC command. If the VTP mode is transparent, VLAN configuration information for normal-range VLANs is also saved in the device running configuration file. VLAN IDs in the extended range are not saved in the VLAN database, but they are stored in the switch running configuration file, and you can save the configuration in the startup configuration file.

VTP version 3 supports propagation of extended-range VLANs. VTP versions 1 and 2 propagate only VLANs 1 to 1005.

When you save the VLAN and VTP configurations in the startup configuration file and reboot the device, the configuration is selected as follows:

- If the VTP mode is transparent in the startup configuration and the VLAN database and the VTP domain name from the VLAN database matches that in the startup configuration file, the VLAN database is ignored (cleared), and the VTP and VLAN configurations in the startup configuration file are used. The VLAN database revision number remains unchanged in the VLAN database.
- If the VTP mode or domain name in the startup configuration do not match the VLAN database, the domain name and VTP mode and configuration for VLAN IDs 1 to 1005 use the VLAN database information.

If you enter an invalid VLAN ID, you receive an error message and do not enter VLAN configuration mode.

Entering the `vlan` command with a VLAN ID enables VLAN configuration mode. When you enter the VLAN ID of an existing VLAN, you do not create a new VLAN, but you can modify VLAN parameters for that VLAN. The specified VLANs are added or modified when you exit the VLAN configuration mode. Only the `shutdown` command (for VLANs 1 to 1005) takes effect immediately.
Although all commands are visible, the only VLAN configuration command that is supported on extended-range VLANs is `remote-span`. For extended-range VLANs, all other characteristics must remain at the default state.

These configuration commands are available in VLAN configuration mode. The `no` form of each command returns the characteristic to its default state:

- **are are-number**—Defines the maximum number of all-routes explorer (ARE) hops for this VLAN. This keyword applies only to TrCRF VLANs. The range is 0 to 13. The default is 7. If no value is entered, 0 is assumed to be the maximum.

- **backupcrf**—Specifies the backup CRF mode. This keyword applies only to TrCRF VLANs.
  - **enable**—Backup CRF mode for this VLAN.
  - **disable**—Backup CRF mode for this VLAN (the default).

- **bridge {bridge-number | type}**—Specifies the logical distributed source-routing bridge, the bridge that interconnects all logical rings that have this VLAN as a parent VLAN in FDDI-NET, Token Ring-NET, and TrBRF VLANs. The range is 0 to 15. The default bridge number is 0 (no source-routing bridge) for FDDI-NET, TrBRF, and Token Ring-NET VLANs. The `type` keyword applies only to TrCRF VLANs and is one of these:
  - **srb**—Source-route bridging
  - **srt**—Source-route transparent bridging VLAN

- **exit**—Applies changes, increments the VLAN database revision number (VLANs 1 to 1005 only), and exits VLAN configuration mode.

- **media**—Defines the VLAN media type and is one of these:

  - **ethernet**—Ethernet media type (the default).
  - **fd-net**—FDDI network entity title (NET) media type.
  - **fddi**—FDDI media type.
  - **tokenring**—Token Ring media type if the VTP v2 mode is disabled, or TrCRF if the VTP Version 2 (v) mode is enabled.
  - **tr-net**—Token Ring network entity title (NET) media type if the VTP v2 mode is disabled or TrBRF media type if the VTP v2 mode is enabled.

  See the table that follows for valid commands and syntax for different media types.

- **name vlan-name**—Names the VLAN with an ASCII string from 1 to 32 characters that must be unique within the administrative domain. The default is VLANxxxx where xxxx represents four numeric digits (including leading zeros) equal to the VLAN ID number.

---

**Note** The device supports only Ethernet ports. You configure only FDDI and Token Ring media-specific characteristics for VLAN Trunking Protocol (VTP) global advertisements to other devices. These VLANs are locally suspended.
• **no**—Negates a command or returns it to the default setting.

• **parent parent-vlan-id**— Specifies the parent VLAN of an existing FDDI, Token Ring, or TrCRF VLAN. This parameter identifies the TrBRF to which a TrCRF belongs and is required when defining a TrCRF. The range is 0 to 1005. The default parent VLAN ID is 0 (no parent VLAN) for FDDI and Token Ring VLANs. For both Token Ring and TrCRF VLANs, the parent VLAN ID must already exist in the database and be associated with a Token Ring-NET or TrBRF VLAN.

• **remote-span**—Configures the VLAN as a Remote SPAN (RSPAN) VLAN. When the RSPAN feature is added to an existing VLAN, the VLAN is first deleted and is then recreated with the RSPAN feature. Any access ports are deactivated until the RSPAN feature is removed. If VTP is enabled, the new RSPAN VLAN is propagated by VTP for VLAN IDs that are lower than 1024. Learning is disabled on the VLAN.

• **ring ring-number**— Defines the logical ring for an FDDI, Token Ring, or TrCRF VLAN. The range is 1 to 4095. The default for Token Ring VLANs is 0. For FDDI VLANs, there is no default.

• **said said-value**— Specifies the security association identifier (SAID) as documented in IEEE 802.10. The range is 1 to 4294967294, and the number must be unique within the administrative domain. The default value is 100000 plus the VLAN ID number.

• **shutdown**—Shuts down VLAN switching on the VLAN. This command takes effect immediately. Other commands take effect when you exit VLAN configuration mode.

• **state**—Specifies the VLAN state:
  • **active** means the VLAN is operational (the default).
  • **suspend** means the VLAN is suspended. Suspended VLANs do not pass packets.

• **ste ste-number**— Defines the maximum number of spanning-tree explorer (STE) hops. This keyword applies only to TrCRF VLANs. The range is 0 to 13. The default is 7.

• **stp type**— Defines the spanning-tree type for FDDI-NET, Token Ring-NET, or TrBRF VLANs. For FDDI-NET VLANs, the default STP type is ieee. For Token Ring-NET VLANs, the default STP type is ibm. For FDDI and Token Ring VLANs, the default is no type specified.
  • **ieee**—IEEE Ethernet STP running source-route transparent (SRT) bridging.
  • **ibm**—IBM STP running source-route bridging (SRB).
  • **auto**—STP running a combination of source-route transparent bridging (IEEE) and source-route bridging (IBM).

• **tb-vlan1 tb-vlan1-id and tb-vlan2 tb-vlan2-id**— Specifies the first and second VLAN to which this VLAN is translationally bridged. Translational VLANs translate FDDI or Token Ring to Ethernet, for example. The range is 0 to 1005. If no value is specified, 0 (no transitional bridging) is assumed.

<table>
<thead>
<tr>
<th>Media Type</th>
<th>Valid Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet</td>
<td>name vlan-name, media ethernet, state {suspend</td>
</tr>
<tr>
<td>Media Type</td>
<td>Valid Syntax</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>FDDI</td>
<td>name vlan-name, media fddi, state {suspend</td>
</tr>
<tr>
<td>FDDI-NET</td>
<td>name vlan-name, media fd-net , state {suspend</td>
</tr>
<tr>
<td>Token Ring</td>
<td>VTP v1 mode is enabled. name vlan-name, media tokenring, state {suspend</td>
</tr>
<tr>
<td>Token Ring concentrator relay function (TrCRF)</td>
<td>VTP v2 mode is enabled. name vlan-name, media tokenring, state {suspend</td>
</tr>
<tr>
<td>Token Ring-NET</td>
<td>VTP v1 mode is enabled. name vlan-name, media tr-net, state {suspend</td>
</tr>
<tr>
<td>Token Ring bridge relay function (TrBRF)</td>
<td>VTP v2 mode is enabled. name vlan-name, media tr-net, state {suspend</td>
</tr>
</tbody>
</table>

The following table describes the rules for configuring VLANs:
### Table 9: VLAN Configuration Rules

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>VTP v2 mode is enabled, and you are configuring a TrCRF VLAN media type.</td>
<td>Specify a parent VLAN ID of a TrBRF that already exists in the database. Specify a ring number. Do not leave this field blank.</td>
</tr>
<tr>
<td></td>
<td>Specify unique ring numbers when TrCRF VLANs have the same parent VLAN ID. Only one backup concentrator relay function (CRF) can be enabled.</td>
</tr>
<tr>
<td>VTP v2 mode is enabled, and you are configuring VLANs other than TrCRF media type.</td>
<td>Do not specify a backup CRF.</td>
</tr>
<tr>
<td>VTP v2 mode is enabled, and you are configuring a TrBRF VLAN media type.</td>
<td>Specify a bridge number. Do not leave this field blank.</td>
</tr>
<tr>
<td>VTP v1 mode is enabled.</td>
<td>No VLAN can have an STP type set to auto. This rule applies to Ethernet, FDDI, FDDI-NET, Token Ring, and Token Ring-NET VLANs.</td>
</tr>
<tr>
<td>Add a VLAN that requires translational bridging (values are not set to zero).</td>
<td>The translational bridging VLAN IDs that are used must already exist in the database. The translational bridging VLAN IDs that a configuration points to must also contain a pointer to the original VLAN in one of the translational bridging parameters (for example, Ethernet points to FDDI, and FDDI points to Ethernet). The translational bridging VLAN IDs that a configuration points to must be different media types than the original VLAN (for example, Ethernet can point to Token Ring). If both translational bridging VLAN IDs are configured, these VLANs must be different media types (for example, Ethernet can point to FDDI and Token Ring).</td>
</tr>
</tbody>
</table>

This example shows how to add an Ethernet VLAN with default media characteristics. The default includes a `vlan-name` of VLAN xxxx, where xxxx represents four numeric digits (including leading zeros) equal to the VLAN ID number. The default media is ethernet; the state is active. The default said-value is 100000 plus the VLAN ID; the mtu-size variable is 1500; the stp-type is ieee. When you enter the `exit` VLAN configuration command, the VLAN is added if it did not already exist; otherwise, this command does nothing.

This example shows how to create a new VLAN with all default characteristics and enter VLAN configuration mode:

```
Device(config)# vlan 200
Device(config-vlan)# exit
Device(config)#
```
This example shows how to create a new extended-range VLAN with all the default characteristics, to enter VLAN configuration mode, and to save the new VLAN in the device startup configuration file:

```
Device(config)# vlan 2000
Device(config-vlan)# end
Device# copy running-config startup config
```

You can verify your setting by entering the `show vlan` privileged EXEC command.
**vlan configuration**

To enter the VLAN configuration mode to configure VLAN features, use the `vlan configuration` command.

```
vlan configuration
```

**Command Default**

None

**Command Modes**

Global configuration (config)

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enter the VLAN configuration mode to configure VLAN features, with the VLAN ID being 2:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# vlan configuration 2
```
vlan access-map

To create or modify a VLAN map entry for VLAN packet filtering, and change the mode to the VLAN access-map configuration, use the `vlan access-map` command in global configuration mode on the switch stack or on a standalone switch. To delete a VLAN map entry, use the `no` form of this command.

```
vlan access-map name [number]
no vlan access-map name [number]
```

**Note**
This command is not supported on switches running the LAN Base feature set.

**Syntax Description**

- `name` Name of the VLAN map.
- `number` (Optional) The sequence number of the map entry that you want to create or modify (0 to 65535). If you are creating a VLAN map and the sequence number is not specified, it is automatically assigned in increments of 10, starting from 10. This number is the sequence to insert to, or delete from, a VLAN access-map entry.

**Command Default**
There are no VLAN map entries and no VLAN maps applied to a VLAN.

**Command Modes**
Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

In global configuration mode, use this command to create or modify a VLAN map. This entry changes the mode to VLAN access-map configuration, where you can use the `match` access-map configuration command to specify the access lists for IP or non-IP traffic to match and use the `action` command to set whether a match causes the packet to be forwarded or dropped.

In VLAN access-map configuration mode, these commands are available:

- `action`—Sets the action to be taken (forward or drop).
- `default`—Sets a command to its defaults.
- `exit`—Exits from VLAN access-map configuration mode.
- `match`—Sets the values to match (IP address or MAC address).
- `no`—Negates a command or set its defaults.

When you do not specify an entry number (sequence number), it is added to the end of the map.

There can be only one VLAN map per VLAN and it is applied as packets are received by a VLAN.

You can use the `no vlan access-map name [number]` command with a sequence number to delete a single entry.
Use the **vlan filter** interface configuration command to apply a VLAN map to one or more VLANs.

For more information about VLAN map entries, see the software configuration guide for this release.

This example shows how to create a VLAN map named `vac1` and apply matching conditions and actions to it. If no other entries already exist in the map, this will be entry 10.

```
Device(config)# vlan access-map vac1
Device(config-access-map)# match ip address acl1
Device(config-access-map)# action forward
```

This example shows how to delete VLAN map `vac1`:

```
Device(config)# no vlan access-map vac1
```
To apply a VLAN map to one or more VLANs, use the `vlan filter` command in global configuration mode on the switch stack or on a standalone switch. To remove the map, use the `no` form of this command.

```
vlan filter mapname vlan-list {list|all}
no vlan filter mapname vlan-list {list|all}
```

**Note**
This command is not supported on switches running the LAN Base feature set.

**Syntax Description**
- `mapname`: Name of the VLAN map entry.
- `vlan-list`: Specifies which VLANs to apply the map to.
- `list`: The list of one or more VLANs in the form tt, uu-vv, xx, yy-zz, where spaces around commas and dashes are optional. The range is 1 to 4094.
- `all`: Adds the map to all VLANs.

**Command Default**
There are no VLAN filters.

**Command Modes**
Global configuration

**Command History**
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
To avoid accidentally dropping too many packets and disabling connectivity in the middle of the configuration process, we recommend that you completely define the VLAN access map before applying it to a VLAN.

For more information about VLAN map entries, see the software configuration guide for this release.

This example applies VLAN map entry `map1` to VLANs 20 and 30:
```
Device(config)# vlan filter map1 vlan-list 20, 30
```

This example shows how to delete VLAN map entry `map1` from VLAN 20:
```
Device(config)# no vlan filter map1 vlan-list 20
```

You can verify your settings by entering the `show vlan filter` privileged EXEC command.
**vlan group**

To create or modify a VLAN group, use the `vlan group` command in global configuration mode. To remove a VLAN list from the VLAN group, use the `no` form of this command.

```
vlan group group-name vlan-list
no vlan group group-name vlan-list
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>group-name</code></td>
<td>Name of the VLAN group. The group name may contain up to 32 characters and must begin with a letter.</td>
</tr>
<tr>
<td><code>vlan-list</code></td>
<td>Specifies one or more VLANs to be added to the VLAN group. The <code>vlan-list</code> argument can be a single VLAN ID, a list of VLAN IDs, or VLAN ID range. Multiple entries are separated by a hyphen (-) or a comma (,).</td>
</tr>
</tbody>
</table>

**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 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If the named VLAN group does not exist, the `vlan group` command creates the group and maps the specified VLAN list to the group. If the named VLAN group exists, the specified VLAN list is mapped to the group.

The `no` form of the `vlan group` command removes the specified VLAN list from the VLAN group. When you remove the last VLAN from the VLAN group, the VLAN group is deleted.

A maximum of 100 VLAN groups can be configured, and a maximum of 4094 VLANs can be mapped to a VLAN group.

This example shows how to map VLANs 7 through 9 and 11 to a VLAN group:

```
Device(config)# vlan group group1 vlan-list 7-9,11
```

This example shows how to remove VLAN 7 from the VLAN group:

```
Device(config)# no vlan group group1 vlan-list 7
```
wgb broadcast-tagging

To configure WGB broadcast tagging for a wireless policy profile, use the `wgb broadcast-tagging` command.

**wgb broadcast-tagging**

**Command Default**

None

**Command Modes**

config-wireless-policy

**Command History**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enable WGB broadcast tagging for a wireless policy profile:

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

To configure WGB VLAN client support for a WLAN policy profile, use the `wgb vlan` command.

```
wgb vlan
```

**Command Default**

None

**Command Modes**

config-wireless-policy

**Command History**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enable WGB VLAN client support for the WLAN policy profile named `wlan1-policy-profile`:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless profile policy wlan1-policy-profile
Device(config-wireless-policy)# wgb vlan
```
whitelist acl

To configure the whitelist ACL, use the `whitelist acl` command.

```
whitelist acl {standard_acl_value | extended_acl_value | acl_name}
```

**Syntax Description**

- **standard_acl_value**  
  Specifies the standard access list. Range is from 1 to 199.

- **extended_acl_value**  
  Specifies the extended access list. Range is from 1300 to 2699.

- **acl_name**  
  Specifies the named access list.

**Command Default**

None

**Command Modes**

ET-Analytics configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>3.2SE</td>
<td></td>
</tr>
</tbody>
</table>

This example shows how to enable in-active timer in the ET-Analytics configuration mode:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# et-analytics
Device(config-et-analytics)# whitelist acl eta-whitelist
Device(config-et-analytics)# ip access-list extended eta-whitelist
Device(config-ext-nacl)# permit udp any any eq tftp
Device(config-ext-nacl)# end
```
config wlan assisted-roaming

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

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

**Syntax Description**

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

**Command Default**

The 802.11k neighbor list is enabled for all WLANs.

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

**Usage Guidelines**

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

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

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

To configure a wireless AAA policy, use the **wireless aaa policy** command.

```plaintext
wireless aaa policy aaa-policy
```

**Syntax Description**

- `aaa-policy` Name of the wireless AAA policy.

**Command Default**

None

**Command Modes**

Global configuration (config)

**Command History**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure a wireless AAA policy named `aaa-policy-test`

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless aaa policy aaa-policy-test
```
To configure a new AAA policy, use the `wireless aaa policy` command.

```
wireless aaa policy aaa-policy-name
```

**Syntax Description**

- `aaa-policy-name` AAA policy name.

**Command Default**

None

**Command Modes**

Global configuration (config)

**Command History**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure a AAA policy name:

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

To enable broadcast support on a VLAN, use the **wireless broadcast vlan** command in global configuration mode. To disable Ethernet broadcast support, use the **no** form of the command.

```
wireless broadcast vlan [vlan-id]
no wireless broadcast vlan [vlan-id]
```

**Syntax Description**
- `vlan-id` (Optional) Specifies the VLAN ID to enable broadcast support to that VLAN. The value ranges from 1 to 4095.

**Command Default**
None

**Command Modes**
Global configuration mode

**Command History**
- **Release** 3.2SE
  - Modification: This command was introduced.

**Usage Guidelines**
Use this command in the global configuration mode only.

This example shows how to enable broadcasting on VLAN 20:

```
Device(config)# wireless broadcast vlan 20
```
wireless client

To configure client parameters, use the **wireless client** command in global configuration mode.

```
wireless client {association limit assoc-number interval interval|band-select {client-mid-rssi rssi|client-rssi rssi|cycle-count count|cycle-threshold threshold|expire dual-band timeout|expire suppression timeout|fast-ssid-change|max-user-login max-user-login|notification {interval time|join-failure aathreshold percentage|roam-failure threshold percentage} |timers auth-timeout seconds |user-timeout user-timeout}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>association limit assoc-number interval interval</td>
<td>Enables association request limit per access point slot at a given interval and configures the association request limit interval. You can configure number of association request per access point slot at a given interval from one through 100. You can configure client association request limit interval from 100 through 10000 milliseconds.</td>
</tr>
<tr>
<td>band-select</td>
<td>Configures the band select options for the client.</td>
</tr>
<tr>
<td>client-mid-rssi rssi</td>
<td>Sets the client mid-rssi threshold for band select. The minimum dBm of a client RSSI to respond to probe is between -90 and -20.</td>
</tr>
<tr>
<td>client-rssi rssi</td>
<td>Sets the client received signal strength indicator (RSSI) threshold for band select. The minimum dBm of a client RSSI to respond to probe is between -90 and -20.</td>
</tr>
<tr>
<td>cycle-count count</td>
<td>Sets the band select probe cycle count. You can configure the cycle count from 1 to 10.</td>
</tr>
<tr>
<td>cycle-threshold threshold</td>
<td>Sets the time threshold for a new scanning cycle. You can configure the cycle threshold from 1 to 1000 milliseconds.</td>
</tr>
<tr>
<td>expire dual-band timeout</td>
<td>Sets the timeout before stopping to try to push a given client to the 5-GHz band. You can configure the timeout from 10 to 300 seconds, and the default value is 60 seconds.</td>
</tr>
<tr>
<td>expire suppression timeout</td>
<td>Sets the expiration time for pruning previously known dual-band clients. You can configure the suppression from 10 to 200 seconds, and the default timeout value is 20 seconds.</td>
</tr>
<tr>
<td>fast-ssid-change</td>
<td>Enables the fast SSID change for mobile stations.</td>
</tr>
<tr>
<td>max-user-login max-user-login</td>
<td>Configures the maximum number of login sessions for a user.</td>
</tr>
</tbody>
</table>
### wireless client

<table>
<thead>
<tr>
<th>Command Default</th>
<th>No default behavior or values.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>Global configuration</td>
</tr>
<tr>
<td>Command History</td>
<td></td>
</tr>
<tr>
<td>Release</td>
<td>Modification</td>
</tr>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
<td>This command was modified. The client-mid-rssi, notification, and fast-ssid-change keywords were added. The user-timeout keyword was deleted.</td>
</tr>
</tbody>
</table>

This example shows how to set the probe cycle count for band select to 8:

```
Device# configure terminal
Device(config)# wireless client band-select cycle-count 8
Device(config)# end
```

This example shows how to set the time threshold for a new scanning cycle with threshold value of 700 milliseconds:

```
Device# configure terminal
Device(config)# wireless client band-select cycle-threshold 700
Device(config)# end
```

This example shows how to suppress dual-band clients from the dual-band database after 70 seconds:

```
Device# configure terminal
Device(config)# wireless client band-select expire suppression 70
Device(config)# end
```
**wireless client mac-address**

To configure the wireless client settings, use the `wireless client mac-address` command in global configuration mode.

```plaintext
wireless client mac-address mac-addr ccx
clear-reports|clear-results|default-gw-ping|dhcp-test|dns-ping|dns-resolve hostname
host-name|get-client-capability|get-manufacturer-info|get-operating-parameters|get-profiles|log-request
{roam|rsna|syslog}|send-message message-id|stats-request measurement-duration
dot11|security|test-abort|test-association ssid bssid dot11 channel|test-dot1x [profile-id] bssid
channel|test-profile {any|profile-id}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac-addr</td>
<td>MAC address of the client.</td>
</tr>
<tr>
<td>ccx</td>
<td>Cisco client extension (CCX).</td>
</tr>
<tr>
<td>clear-reports</td>
<td>Clears the client reporting information.</td>
</tr>
<tr>
<td>clear-results</td>
<td>Clears the test results on the controller.</td>
</tr>
<tr>
<td>default-gw-ping</td>
<td>Sends a request to the client to perform the default gateway ping test.</td>
</tr>
<tr>
<td>dhcp-test</td>
<td>Sends a request to the client to perform the DHCP test.</td>
</tr>
<tr>
<td>dns-ping</td>
<td>Sends a request to the client to perform the Domain Name System (DNS) server IP address ping test.</td>
</tr>
<tr>
<td>dns-resolve hostname</td>
<td>Sends a request to the client to perform the Domain Name System (DNS) resolution test to the specified hostname.</td>
</tr>
<tr>
<td>host-name</td>
<td>Sends a request to the client to perform the Domain Name System (DNS) server IP address ping test.</td>
</tr>
<tr>
<td>get-client-capability</td>
<td>Sends a request to the client to send its capability information.</td>
</tr>
<tr>
<td>get-manufacturer-info</td>
<td>Sends a request to the client to send the manufacturer's information.</td>
</tr>
<tr>
<td>get-operating-parameters</td>
<td>Sends a request to the client to send its current operating parameters.</td>
</tr>
<tr>
<td>get-profiles</td>
<td>Sends a request to the client to send its profiles.</td>
</tr>
<tr>
<td>log-request</td>
<td>Configures a CCX log request for a specified client device.</td>
</tr>
<tr>
<td>roam</td>
<td>(Optional) Specifies the request to specify the client CCX roaming log</td>
</tr>
<tr>
<td>rsna</td>
<td>(Optional) Specifies the request to specify the client CCX RSNA log.</td>
</tr>
<tr>
<td>syslog</td>
<td>(Optional) Specifies the request to specify the client CCX system log.</td>
</tr>
</tbody>
</table>
send-message message-id
Sends a message to the client.

Message type that involves one of the following:

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>stats-request</td>
<td>Sends a request for statistics.</td>
</tr>
<tr>
<td>measurement-duration</td>
<td>Optional) Specifies dot11 counters.</td>
</tr>
<tr>
<td>dot11</td>
<td>(Optional) Specifies security counters.</td>
</tr>
<tr>
<td>test-abort</td>
<td>Sends a request to the client to abort the current test.</td>
</tr>
<tr>
<td>test-association</td>
<td>Sends a request to the client to perform the association test.</td>
</tr>
<tr>
<td>ssid bssid dot11 channel</td>
<td>Sends a request to the client to perform the 802.1x test.</td>
</tr>
<tr>
<td>test-dot1x</td>
<td>Sends a request to the client to perform the 802.1x test.</td>
</tr>
<tr>
<td>profile-id</td>
<td>(Optional) Test profile name.</td>
</tr>
<tr>
<td>bssid</td>
<td>Basic SSID.</td>
</tr>
<tr>
<td>dot11</td>
<td>Specifies the 802.11a, 802.11b, or 802.11g network.</td>
</tr>
<tr>
<td>channel</td>
<td>Channel number.</td>
</tr>
<tr>
<td>test-profile</td>
<td>Sends a request to the client to perform the profile redirect test.</td>
</tr>
<tr>
<td>any</td>
<td>Sends a request to the client to perform the profile redirect test.</td>
</tr>
<tr>
<td>profile-id</td>
<td>Test profile name.</td>
</tr>
</tbody>
</table>

**Note** The profile ID should be from one of the client profiles for which client reporting is enabled.

**Command Default**
No default behavior or values.

**Command Modes**
Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
The **default-gw-ping** test does not require the client to use the diagnostic channel.

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

```
Device# configure terminal
```
wireless client mac-address

Device(config)# wireless client mac-address 00:1f:ca:cf:b6:60 ccx clear-reports
Device(config)# end
wireless config validate

To validate whether the wireless configuration is complete and consistent (all the functional profiles and tags are defined, and all the associations are complete and consistent), use the `wireless config validate` command in privileged EXEC mode.

**wireless config validate**

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

**Command Default**
None

**Command Modes**
Privileged EXEC (#)

**Command History**

<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>

**Usage Guidelines**

In Cisco vEWLC, the wireless configuration is built using a collection of profiles, with each profile defining a functional block. These functional blocks are defined independently and is used to realize well-defined associations through intent based work-flows in building the wireless LAN. Such flexibility of modularizing the functional blocks requires the administrator to ensure that all associations are consistent and complete.

To ensure completeness and consistency of the wireless configuration, a configuration validation library is used to validate the configuration definitions across tables. The `wireless config validate` exec command is introduced from this release to validate the wireless configuration and report inconsistencies, if any, using contextual error message that is visible in btrace infra and on the console (if console logging is enabled). This command calls out any inconsistencies (unresolved associations) enabling you to realize a functional wireless LAN.

Use the following command to direct the output to a file: `show logging | redirect bootflash: filename`.

The following set of wireless configurations are validated:

<table>
<thead>
<tr>
<th>RF tag</th>
<th>Site tag</th>
<th>Policy tag</th>
<th>Policy profile</th>
<th>Flex profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>site-tag</td>
<td>flex-profile</td>
<td>wlan profile</td>
<td>IPv4 ACL name</td>
<td>VLAN ACL</td>
</tr>
<tr>
<td>poliy-tag</td>
<td>ap-profile</td>
<td>policy profile</td>
<td>Fabric name</td>
<td>ACL-policy</td>
</tr>
<tr>
<td>rf-tag</td>
<td>---</td>
<td>---</td>
<td>service-policy input and output name</td>
<td>RF Policy (5GHz and 24GHz)</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>service-policy input and client output name</td>
<td>---</td>
</tr>
</tbody>
</table>
Example

The following is sample output from the **wireless config validate** command

```
Device# wireless config validate

```
wireless fabric control-plane

To configure a control plane name applicable to the wireless fabric mode, use the `wireless fabric control-plane` command.

```
wireless fabric control-plane control-plane-name
```

**Syntax Description**

- `control-plane-name` Control plane name that is applicable to the wireless fabric mode.

**Command Default**

None

**Command Modes**

Global configuration (config)

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If you do not provide a control plane name, the default-control-plane, which is auto-generated, is used.

**Examples**

The following example shows how to configure a control plane name:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless fabric control-plane test-control-plane
```
wireless fabric

To enable SD-Access Wireless globally on the controller, use the `wireless fabric` command.

```
wireless fabric
```

**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 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

This example shows how to enable SD-Access wireless globally on the controller:

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

To configure wireless fabric name VXLAN ID (VNID) map, use the `wireless fabric name` command.

```
wireless fabric [control-plane control-plane-name] | [name vnid-map-name l2-vnid id {control-plane control-plane-name | l3-vnid id} ip {ipv-addr netmask-addr | ipv6-addr netmask-addr} {control-plane control-plane-name}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>control-plane control-plane-name</code></td>
<td>Configure the control plane details.</td>
</tr>
<tr>
<td><code>name vnid-map-name</code></td>
<td>Configure the wireless fabric name</td>
</tr>
<tr>
<td><code>l2-vnid id</code></td>
<td>Configure the Layer 2 VNID. Valid range is 0 to 16777215.</td>
</tr>
<tr>
<td><code>l3-vnid id</code></td>
<td>Configure the Layer 3 VNID. Valid range is 0 to 16777215.</td>
</tr>
<tr>
<td>`ip {ipv4-addr netmask-addr</td>
<td>ipv6-addr netmask-addr}`</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

Global configuration (config)

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure MAP server per VNID for Layer 2 and Layer 3:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless fabric name vnid-map l2-vnid 2 l3-vnid 10 ip 209.165.200.224 255.255.255.224
```
## wireless load-balancing

To globally configure aggressive load balancing on the controller, use the `wireless load-balancing` command in global configuration mode.

```
wireless load-balancing {denial denial-count|window client-count}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>denial denial-count</td>
<td>Specifies the number of association denials during load balancing. Maximum number of association denials during load balancing is from 1 to 10 and the default value is 3.</td>
</tr>
<tr>
<td>window client-count</td>
<td>Specifies the aggressive load balancing client window, with the number of clients needed to trigger aggressive load balancing on a given access point. Aggressive load balancing client window with the number of clients is from 0 to 20 and the default value is 5.</td>
</tr>
</tbody>
</table>

### Command Default

Disabled.

### Command Modes

Global configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Load-balancing-enabled WLANs do not support time-sensitive applications like voice and video because of roaming delays.

When you use Cisco 7921 and 7920 Wireless IP Phones with controllers, make sure that aggressive load balancing is disabled on the voice WLANs for each controller. Otherwise, the initial roam attempt by the phone might fail, causing a disruption in the audio path.

This example shows how to configure association denials during load balancing:

```
Device# configure terminal
Device(config)# wireless load-balancing denial 5
Device(config)# end
```
wireless macro-micro steering transition-threshold

To configure micro-macro transition thresholds, use the `wireless macro-micro steering transition-threshold` command.

```
wireless macro-micro steering transition-threshold {balancing-window |client count number-clients }
{macro-to-micro |micro-to-macro RSSI in dBm}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>balancing-window</td>
<td>Active instance of the configuration in Route-processor slot 0.</td>
</tr>
<tr>
<td>client</td>
<td>Standby instance of the configuration in Route-processor slot 0.</td>
</tr>
<tr>
<td>number-clients</td>
<td>Valid range is 0 to 65535 clients.</td>
</tr>
<tr>
<td>macro-to-micro</td>
<td>Configures the macro to micro transition RSSI.</td>
</tr>
<tr>
<td>micro-to-macro</td>
<td>Configures micro-macro client load balancing window.</td>
</tr>
<tr>
<td>RSSI in dBm</td>
<td>RSSI in dBm. Valid range is –128 to 0.</td>
</tr>
</tbody>
</table>

### Command Default

None

### Command Modes

Global configuration (config)

### Command History

<table>
<thead>
<tr>
<th>Modification</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to configure balancing-window:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless macro-micro steering transition-threshold balancing-window number-of-clients
```
To configure various parameters, use the **wireless media-stream** command.

```plaintext
wireless media-stream group groupName [startipAddr endipAddr]
wireless media-stream group { avg-packet-size default exit max-bandwidth no policy qos }
wireless media-stream { multicast-direct message [{ phone phone | URL URL | Notes Notes | Email Email }]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>group</code></td>
<td>Configure multicast-direct status for a group.</td>
</tr>
<tr>
<td><code>groupName</code></td>
<td>Specifies the start IP Address for the group.</td>
</tr>
<tr>
<td><code>startipAddr</code></td>
<td>Specifies the End IP Address for the group.</td>
</tr>
<tr>
<td><code>endipAddr</code></td>
<td></td>
</tr>
<tr>
<td><code>avg-packet-size</code></td>
<td>Configure average packet size. The values can range between 100 to 1500.</td>
</tr>
<tr>
<td><code>default</code></td>
<td>Set a command to its defaults.</td>
</tr>
<tr>
<td><code>exit</code></td>
<td>Exit sub-mode.</td>
</tr>
<tr>
<td><code>max-bandwidth</code></td>
<td>Configure maximum expected stream bandwidth in Kbps. The values can range between 1 to 35000 kbps.</td>
</tr>
<tr>
<td><code>no</code></td>
<td>Negate a command or set its defaults.</td>
</tr>
<tr>
<td><code>policy</code></td>
<td>Configure media stream admission policy.</td>
</tr>
<tr>
<td><code>qos</code></td>
<td>You can choose either of these options:</td>
</tr>
<tr>
<td><code>multicast-direct</code></td>
<td>• admit - Allow traffic for the media stream group.</td>
</tr>
<tr>
<td><code>message</code></td>
<td>• deny - Deny traffic for the media stream group.</td>
</tr>
<tr>
<td><code>phone</code></td>
<td>Configure over the air QoS class, `&lt;video'&gt; ONLY.</td>
</tr>
<tr>
<td><code>URL</code></td>
<td>Configure multicast-direct status.</td>
</tr>
<tr>
<td><code>URL</code></td>
<td>Configure Session Announcement Message.</td>
</tr>
<tr>
<td><code>Notes</code></td>
<td>Configure Session Announcement Phone number.</td>
</tr>
<tr>
<td><code>Email</code></td>
<td>Configure Session Announcement URL.</td>
</tr>
<tr>
<td><code>Notes</code></td>
<td>Configure Session Announcement notes.</td>
</tr>
<tr>
<td><code>Email</code></td>
<td>Configure Session Announcement Email.</td>
</tr>
</tbody>
</table>
Command Default: Disabled

Command Modes: config

Command History:

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE</td>
<td>This command was modified.</td>
</tr>
<tr>
<td>Gibraltar 16.10.1</td>
<td></td>
</tr>
</tbody>
</table>

Usage Guidelines:

Media-stream multicast-direct requires load-based Call Admission Control (CAC) to run.

Examples:

The following example shows how to configure each media stream and its parameters like expected multicast destination addresses, stream bandwidth consumption and stream priority parameters.

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless media-stream group GROUP1 231.1.1.1 231.1.1.10
```
wireless media-stream message

To configure session announcement message, use the wireless media-stream message command.

```
wireless media-stream message {Email | Notes | URL | phone}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>Configure session announcement e-mail.</td>
</tr>
<tr>
<td>Notes</td>
<td>Configure session announcement notes.</td>
</tr>
<tr>
<td>URL</td>
<td>Configure session announcement URL.</td>
</tr>
<tr>
<td>phone</td>
<td>Configure session announcement phone number.</td>
</tr>
</tbody>
</table>

### Command Default

None

### Command Modes

Global configuration (config)

### 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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

When a media stream is refused (due to bandwidth constraints), a message can be sent to the user. These parameters configure the messages to send IT support e-mail address, notes (message to display explaining why the stream was refused), URL to which the user can be redirected to and the phone number that the user can call about the refused stream.

### Examples

The following example shows how to configure a session announcement URL:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless media-stream message URL www.example.com
```
wireless media-stream multicast-direct

To configure multicast-direct status, use the `media-stream multicast-direct` command. To remove the multicast-direct status, use the `no` form of the command.

```
no wireless media-stream multicast-direct
```

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>config</td>
</tr>
<tr>
<td>Usage Guidelines</td>
<td>Media stream multicast-direct requires load based Call Admission Control (CAC) to run. WLAN quality of service (QoS) needs to be set to either gold or platinum.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure multicast-direct for a wireless LAN media stream.

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless media-stream multicast-direct
```
**wireless mesh alarm association count**

To configure the mesh alarm association count, use the `wireless mesh alarm association count count` command.

**wireless mesh alarm association count count**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>count</td>
<td>Number of alarm associations. The valid range is between 1 and 30.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>config</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<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>

**Examples**

The following example shows how to configure the mesh alarm association count:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless profile policy wireless mesh alarm association count 10
```
wireless mesh alarm high-snr

To configure the mesh alarm high-snr value, use the **wireless mesh alarm high-snr** command.

```
wired mesh alarm high-snr high-snr
```

**Syntax Description**

- `high-snr` Set the high-snr value. The valid range is between 31 and 100.

**Command Default**

None

**Command Modes**

- config

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure the mesh high-snr:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless profile policy wireless mesh alarm high-snr 75
```
wireless mesh alarm low-snr

To configure the mesh alarm low-snr value, use the `wireless mesh alarm low-snr` command.

```
wireless mesh alarm low-snr low-snr
```

**Syntax Description**

`low-snr`  Set the low-snr value. The valid range is between 1 and 30.

**Command Default**

None

**Command Modes**

config

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure the mesh high-snr:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless profile policy wireless mesh alarm low-snr 5
```
wireless mesh alarm max-children map

To configure the mesh alarm max-children map value, use the `wireless mesh alarm max-children map` command.

```
wireless mesh alarm max-children map max-children
```

**Syntax Description**

`max-children` Set the mesh alarm max-children map parameter. The valid range is between 1 and 50.

**Command Default**

None

**Command Modes**

`config`

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure the mesh alarm max-children map value:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless mesh alarm max-children map 35
```
wireless mesh alarm max-children rap

To configure the mesh alarm max-children rap value, use the `wireless mesh alarm max-children rap` command.

```
wireless mesh alarm max-children rap max-children
```

**Syntax Description**

- **max-children**: Set the mesh alarm max-children rap parameter. The valid range is between 1 and 50.

**Command Default**

None

**Command Modes**

- config

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure the mesh alarm max-children rap value:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless mesh alarm max-children rap 40
```
wireless mesh alarm max-hop

To configure the mesh alarm max-hop parameter, use the `wireless mesh alarm max-hop` command.

```
wireless mesh alarm max-hop max-hop
```

**Syntax Description**

`max-hop` Set the mesh alarm max-hop count. Valid range is between 1 and 16.

**Command Default**

None

**Command Modes**

config

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure the mesh alarm max-hop parameter:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless mesh alarm max-hop 15
```
wireless mesh alarm parent-change count

To configure the max parent-change count value, use the **wireless mesh alarm parent-change count** command.

```
wireless mesh alarm parent-change count count
```

**Syntax Description**

- `count` Set the max parent-change count value. Valid range is between 1 and 30.

**Command Default**

None

**Command Modes**

```
config
```

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure the alarm parent change count value:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless mesh alarm parent-change count 6
```
wireless mesh backhaul bdomain-channels

To configure and allow the Extended UNII B Domain channels for Outdoor mesh APs backhaul radio, use the **wireless mesh backhaul bdomain-channels** command.

**Syntax Description**

- **bdomain-channels** Allows the Extended UNII B Domain channels for Outdoor mesh APs backhaul radio.

  The [no] form of the command disables the use of the Extended UNII B Domain channels by the mesh APs backhaul radio.

**Command Default**

None

**Command Modes**

config

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
</table>
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

**Examples**

The following example shows how to disable the use of Extended UNII B Domain channels by the Outdoor mesh APs backhaul radio:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# no wireless mesh backhaul bdomain-channels
```
wireless mesh backhaul rrm

To configure the mesh backhaul, use the `wireless mesh backhaul` command.

```
wireless mesh backhaul {bdomain-channels | rrm}
```

### Syntax Description

- **backhaul**: Configures the Mesh Backhaul.
- **bdomain-channels**: Allows Extended UNII B Domain channels for Outdoor mesh APs backhaul radio.
- **rrm**: Configures RRM for the mesh backhaul.

### Command Default

None

### Command Modes

- `config`

### 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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to configure RRM for the mesh backhaul:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless mesh backhaul rrm
```
wireless mesh cac

To configure the mesh CAC Mode, use the `wireless mesh cac` command.

```
wireless mesh cac
```

**Syntax Description**

- `cac` Configures the mesh CAC Mode.

**Command Default**

None

**Command Modes**

- config

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
</table>
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1.

**Examples**

The following example shows how to configure the mesh CAC mode:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless mesh cac
```
wireless mesh ethernet-bridging allow-bdpu

To configure STP BPDUs for wired mesh uplink, use the **wireless mesh ethernet-bridging allow-bdpu** command.

**wireless mesh ethernet-bridging allow-bdpu**

**Syntax Description**

<table>
<thead>
<tr>
<th>ethernet-bridging</th>
<th>Configure ethernet bridging.</th>
</tr>
</thead>
<tbody>
<tr>
<td>allow-bdpu</td>
<td>Configures STP BPDUs towards wired MESH uplink.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

config

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure STP BPDUs towards wired MESH uplink:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless mesh ethernet-bridging allow-bdpu
```
wireless mesh security psk provisioning

To provision the mesh security psk parameters, use the **wireless mesh security psk provisioning** command.

```plaintext
wireless mesh security psk provisioning {default_psk | inuse psk-index | key psk-index {0 | 8}} enter-psk-name psk-description
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>provisioning</strong></td>
<td>configuring mesh psk provisioning parameters.</td>
</tr>
<tr>
<td><strong>default_psk</strong></td>
<td>Set the mesh provisioning to the default-psk settings.</td>
</tr>
<tr>
<td><strong>inuse</strong></td>
<td>Configuring the psk inuse index</td>
</tr>
<tr>
<td><strong>psk-index</strong></td>
<td>Enter PSK key index. Valid range is between 1 and 5.</td>
</tr>
<tr>
<td><strong>key</strong></td>
<td>Configure a pre-shared-key</td>
</tr>
<tr>
<td><strong>psk-index</strong></td>
<td>Enter PSK key index. Valid range is between 1 and 5.</td>
</tr>
<tr>
<td><strong>0</strong></td>
<td>Choose to enter an UNENCrypted password.</td>
</tr>
<tr>
<td><strong>8</strong></td>
<td>Choose to enter an AES encrypted password.</td>
</tr>
<tr>
<td><strong>enter-psk-name</strong></td>
<td>Enter a name for the configured psk key.</td>
</tr>
<tr>
<td><strong>psk-description</strong></td>
<td>Enter a description for this key.</td>
</tr>
</tbody>
</table>

### Command Default

None

### Command Modes

**config**

### 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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to provision the default psk key for the mesh security:

```plaintext
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless mesh security psk provisioning default_psk
```
### wireless mesh subset-channel-sync

To configure the subset channel sync for mobility group, use the **wireless mesh subset-channel-sync** command.

**Syntax Description**

**subset-channel-sync**  Configures the subset channel sync for mobility group

**Command Default**

None

**Command Modes**

config

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure subset channel sync for mobility group:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless mesh subset-channel-sync
```
**wireless mobility**

To configure the inter mobility manager, use the `wireless mobility` command.

```
wireless mobility {dscp  value }
```

**Syntax Description**

- `dscp  value` Configures the Mobility inter DSCP value.

**Command Default**

The default DSCP value is 48.

**Command Modes**

Global Configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

This example shows how to configure mobility inter DSCP with an value of 20:

```
Device(config)# wireless mobility dscp 20
```
wireless mobility controller peer-group

To configure mobility peer groups, use the **wireless mobility controller peer-group** command, to remove the configuration, use the **no** form of this command.

**wireless mobility controller peer-group peer-group member IP ip-address mode centralized**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer group</td>
<td>Name of the peer group.</td>
</tr>
<tr>
<td>member IP</td>
<td>Adds a peer group member.</td>
</tr>
<tr>
<td>ip-address</td>
<td>IP address of the peer group member to be added.</td>
</tr>
<tr>
<td>mode centralized</td>
<td>Configures the management mode of the peer group member as centrally managed.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th>The centralized mode is off.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>Global configuration</td>
</tr>
<tr>
<td>Command History</td>
<td></td>
</tr>
<tr>
<td>Release</td>
<td>Modification</td>
</tr>
<tr>
<td>Cisco IOS XE 3.7.0 E</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Device enable
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless mobility controller peer-group peer1 member ip 10.0.0.1 mode centralized
wireless mobility group keepalive

To configure the mobility group parameter and keep alive its ping parameters, use the `wireless mobility group keepalive` command. To remove a mobility group parameter, use the `no` form of the command.

```
wireless mobility group keepalive {count number | interval interval}
no wireless mobility group keepalive {count number | interval interval}
```

**Syntax Description**

- `count number` Number of times that a ping request is sent to a mobility group member before the member is considered unreachable. The range is from 3 to 20. The default is 3.
- `interval interval` Interval of time between each ping request sent to a mobility group member. The range is from 1 to 30 seconds. The default value is 10 seconds.

**Note** For controllers connected through mobility tunnels, ensure that both controllers have the same keepalive interval value.

**Command Default**

3 seconds for `count` and 10 seconds for `interval`.

**Command Modes**

Global Configuration.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The default values for `interval` is ten seconds and the default for `retries` is set to three.

This example shows how to specify the amount of time between each ping request sent to a mobility group member to 10 seconds:

```
Device(config)# wireless mobility group keepalive count 10
```
wireless mobility group mac-address

To configure the MAC address to be used in mobility messages, use the `wireless mobility group mac-address` command.

```
wireless mobility group mac-address mac-addr
```

**Syntax Description**

- `mac-addr`: MAC address to be used in mobility messages.

**Command Default**

None

**Command Modes**

Global configuration (config)

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure a MAC address to be used in mobility messages:

```
Device(config)# wireless mobility group mac-address 00:0d:ed:dd:25:82
```
wireless mobility group member ip

To add or delete users from mobility group member list, use the `wireless mobility group member ip` command. To remove a member from the mobility group, use the `no` form of the command.

```
wireless mobility group member ip ip-address [public-ip public-ip-address] [group group-name]
no wireless mobility group member ip ip-address
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip-address</code></td>
<td>The IP address of the member controller.</td>
</tr>
<tr>
<td><code>public-ip public-ip-address</code></td>
<td>(Optional) Member controller public IP address.</td>
</tr>
<tr>
<td><code>group group-name</code></td>
<td>(Optional) Member controller group name.</td>
</tr>
</tbody>
</table>

**Note**

- This command is used only when the member is behind a NAT. Only static IP NAT is supported.
- This command is used only when the member added in not in the same group as the local mobility controller.

**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 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The mobility group is used when there is more than one Mobility Controller (MC) in a given deployment. The mobility group can be assigned with a name or it can use the default group name. The mobility group members need to be configured on all the members of the group to roam within the group.

This example shows how to add a member in a mobility group:

```
Device(config)# mobility group member ip 10.104.171.101 group TestDocGroup
```
wireless mobility group multicast-address

To configure the multicast IP address for a non-local mobility group, use the `wireless mobility group multicast-address` command.

```
wireless mobility group multicast-address group-name {ipv4 | ipv6} ip-addr
```

**Syntax Description**

- `group-name`: Name of the non-local mobility group.
- `ipv4`: Option to enter the IPv4 address.
- `ipv6`: Option to enter the IPv6 address.
- `ip-addr`: IPv4 or IPv6 address of the non-local mobility group.

**Command Default**

None

**Command Modes**

Global configuration (config)

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure a multicast IPv4 address of the non-local mobility group:

```
Device(config)# wireless mobility group multicast-address Mygroup ipv4 224.0.0.5
```
wireless mobility group name

To configure the mobility domain name, use the `wireless mobility group name` command. To remove the mobility domain name, use the `no` form of the command.

**Note**

If you are configuring the mobility group in a network where network address translation (NAT) is enabled, enter the IP address that is sent to the controller from the NAT device rather than the controller’s management interface IP address. Otherwise, mobility will fail among controllers in the mobility group.

```plaintext
wireless mobility group name  domain-name
no wireless mobility group name
```

**Syntax Description**

- `domain-name` Creates a mobility group by entering this command. The domain name can be up to 31 case-sensitive characters.

**Command Default**

Default.

**Command Modes**

Global Configuration.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

This example shows how to configure a mobility domain name lab1:

```plaintext
Device(config)# mobility group domain lab1
```
wireless mobility multicast ipv4

To configure multicast IPv4 address for the local mobility group, use the `wireless mobility multicast ipv4` command.

```
wireless mobility multicast ipv4 ipv4-addr
```

**Syntax Description**

- `ipv4-addr` Enter the multicast IPv4 address for the local mobility group.

**Command Default**

None

**Command Modes**

Global configuration (config)

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure multicast IPv4 address for the local mobility group:

```
Device(config)# wireless mobility multicast ipv4 224.0.0.4
```
wireless mobility mac-address

To configure the MAC address to be used in mobility messages, use the `wireless mobility mac-address` command.

```
wireless mobility mac-address mac-address
```

**Syntax Description**

- `mac-address` MAC address to be used in mobility messages.

**Command Default**

None

**Command Modes**

Global configuration (config)

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure a MAC address to be used in mobility messages:

```
Device(config)# wireless mobility mac-address 00:0d:bd:5e:9f:00
```
wireless multicast

To configure Ethernet multicast parameters, use the **wireless multicast** command.

\[ \text{wireless multicast } \{ \text{i}pv4-\text{address} \mid \text{ipv6 ipv6-address} \mid \text{non-ip } \{ \text{vlan} \text{ vlan-id} \} \} \]

**Syntax Description**

- **ipv4-address** 
  Multicast IPv4 address.

- **ipv6 ipv6-address** 
  Multicast IPv6 address.

- **non-ip** 
  Configures non-IP multicast in all VLANs. Wireless multicast must be enabled for the traffic to pass.

- **non-ip vlan vlan-id** 
  Configures non-IP multicast per VLAN. Both wireless multicast and wireless multicast non-IP must be enabled for traffic to pass.
  
  Valid range for VLAN ID is 1 to 4094.

**Command Default**

None

**Command Modes**

Global configuration (config)

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure a non-IP multicast for a VLAN whose ID is 5:

```
Device(config)# wireless multicast non-ip vlan 5
```
wireless profile airtime-fairness

To create a new Cisco ATF policy, use the **wireless profile airtime-fairness** command.

**wireless profile airtime-fairness**  
*atf-policy-name*  
*atf-profile-id*

**Syntax Description**

- **atf-policy-name**  Refers to the ATF profile name.
- **atf-profile-id**  Refers to the ATF profile ID. The range is from 0 to 511.

**Command Default**

None

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>3.2SE</td>
<td></td>
</tr>
</tbody>
</table>

This example shows how to create a new Cisco ATF policy:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless profile airtime-fairness <atf-policy-name> 1
Device(config-config-atf)# weight 5
Device(config-config-atf)# client-sharing
Device(config-config-atf)# end
```
wireless profile ap packet-capture

To configure the wireless AP packet capture profile, use the `wireless profile ap packet-capture` command.

```
wireless profile ap packet-capture packet-capture-profile-name
```

**Syntax Description**

- `packet-capture-profile-name`: AP packet capture profile name.

**Command Default**

None

**Command Modes**

Global configuration (config)

**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>

**Example**

The following example shows how to configure the AP packet capture profile:

```
Device(config)# wireless profile ap packet-capture test1
```
To configure the fabric profile parameters, use the `wireless profile fabric` command.

`wireless profile fabric fabric-profile-name`

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>fabric-profile-name</code></td>
<td>Fabric profile name.</td>
</tr>
<tr>
<td><code>fabric</code></td>
<td>Configure Fabric profile parameters.</td>
</tr>
<tr>
<td><code>profile</code></td>
<td>Configure profile parameters.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

Global configuration (config)

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure the fabric profile parameters:

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

To configure WLAN policy profile, use the `wireless profile policy` command.

```
wireless profile policy policy-profile
```

**Syntax Description**

- `policy-profile` Name of the WLAN policy profile.

**Command Default**

The default profile name is `default-policy-profile`.

**Command Modes**

- Global configuration (config)

**Command History**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure a WLAN policy profile:

```
Device(config)# wireless profile policy mywlan-profile-policy
```
wireless rfid

To set the static radio-frequency identification (RFID) tag data timeout value, use the **wireless rfid** command in global configuration mode.

**wireless rfid timeout** *timeout-value*

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>timeout</td>
<td>Configures the static RFID tag data timeout value.</td>
</tr>
<tr>
<td>timeout-value</td>
<td>RFID tag data timeout value. Valid values range from 60-7200.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

Global configuration (config)

**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>

**Example**

This example shows how to set the static RFID tag data timeout value.

```
Device(config)# wireless rfid timeout 70
```
## wireless security dot1x

To configure IEEE 802.1x global configurations, use the `wireless security dot1x` command.

```
wireless security dot1x [{eapol-key retries retries|timeout milliseconds}|group-key interval sec|identity-request retries retries|timeout seconds|radius [call-station-id] {ap-macaddress|ap-macaddress-ssid|ipaddress|macaddress}|request retries retries|timeout seconds|wep key {index 0|index 3}}]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>eapol-key</code></td>
<td>Configures eapol-key related parameters.</td>
</tr>
<tr>
<td><code>retries retries</code></td>
<td>(Optional) Specifies the maximum number of times (0 to 4 retries) that the</td>
</tr>
<tr>
<td></td>
<td>controller retransmits an EAPOL (WPA) key message to a wireless client.</td>
</tr>
<tr>
<td></td>
<td>The default value is 2.</td>
</tr>
<tr>
<td><code>timeout milliseconds</code></td>
<td>(Optional) Specifies the amount of time (200 to 5000 milliseconds) that the</td>
</tr>
<tr>
<td></td>
<td>controller waits before retransmitting an EAPOL (WPA) key message to a</td>
</tr>
<tr>
<td></td>
<td>wireless client using EAP or WPA/WPA-2 PSK.</td>
</tr>
<tr>
<td></td>
<td>The default value is 1000 milliseconds.</td>
</tr>
<tr>
<td><code>group-key interval sec</code></td>
<td>Configures EAP-broadcast key renew interval time in seconds (120 to 86400</td>
</tr>
<tr>
<td></td>
<td>seconds).</td>
</tr>
<tr>
<td><code>identity-request</code></td>
<td>Configures EAP ID request related parameters.</td>
</tr>
<tr>
<td><code>retries retries</code></td>
<td>(Optional) Specifies the maximum number of times (0 to 4 retries) that the</td>
</tr>
<tr>
<td></td>
<td>controller request the EAP ID.</td>
</tr>
<tr>
<td></td>
<td>The default value is 2.</td>
</tr>
<tr>
<td><code>timeout seconds</code></td>
<td>(Optional) Specifies the amount of time (1 to 120 seconds) that the controller waits before retransmitting an EAP Identity Request message to a wireless client. The default value is 30 seconds.</td>
</tr>
<tr>
<td><code>radius</code></td>
<td>Configures radius messages.</td>
</tr>
<tr>
<td><code>call-station-id</code></td>
<td>(Optional) Configures Call-Station Id sent in radius messages.</td>
</tr>
<tr>
<td><code>ap-macaddress</code></td>
<td>Sets Call Station Id Type to the AP's MAC Address.</td>
</tr>
<tr>
<td><code>ap-macaddress-ssid</code></td>
<td>Sets Call Station Id Type to 'AP MAC address':'SSID'.</td>
</tr>
<tr>
<td><code>ipaddress</code></td>
<td>Sets Call Station Id Type to the system's IP Address.</td>
</tr>
<tr>
<td><code>macaddress</code></td>
<td>Sets Call Station Id Type to the system's MAC Address.</td>
</tr>
<tr>
<td><code>request</code></td>
<td>Configures EAP request related parameters.</td>
</tr>
</tbody>
</table>
For EAP messages other than Identity Requests or EAPOL (WPA) key messages, specifies the maximum number of times (0 to 20 retries) that the controller retransmits the message to a wireless client.

The default value is 2.

### timeout seconds

(Optional) For EAP messages other than Identity Requests or EAPOL (WPA) key messages, specifies the amount of time (1 to 120 seconds) that the controller waits before retransmitting the message to a wireless client.

The default value is 30 seconds.

### wep key

Configures 802.1x WEP related parameters.

- **index 0**: Specifies the WEP key index value as 0
- **index 3**: Specifies the WEP key index value as 3

### Command Default

- Default for eapol-key-timeout: 1 second.
- Default for eapol-key-retries: 2 retries.

### Command Modes

- config

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

None.

This example lists all the commands under `wireless security dot1x`.

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless security dot1x ?
  eapol-key Configure eapol-key related parameters
  group-key Configures EAP-broadcast key renew interval time in seconds
  identity-request Configure EAP ID request related parameters
  radius Configure radius messages
  request Configure EAP request related parameters
  wep Configure 802.1x WEP related parameters
  <cr>
```
**wireless security dot1x radius accounting mac-delimiter**

To configure a MAC delimiter for called-station-ID or a calling-station-ID, use the `wireless security dot1x radius accounting mac-delimiter` command.

To remove MAC delimiter for a called-station-ID or a calling-station-ID, use the `no` form of the command.

```
wireless security dot1x radius accounting mac-delimiter { colon | hyphen | none | single-hyphen }
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>colon</td>
<td>Sets the delimiter to colon.</td>
</tr>
<tr>
<td>hyphen</td>
<td>Sets the delimiter to hyphen.</td>
</tr>
<tr>
<td>none</td>
<td>Disables delimiters.</td>
</tr>
<tr>
<td>single-hyphen</td>
<td>Sets the delimiters to single hyphen.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

Global Configuration Mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.6.0 E</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

This example shows how to configure a MAC delimiter for called-station-ID or a calling-station-ID to colon:

```
Device(config)# wireless security dot1x radius accounting mac-delimiter colon
```
wireless security dot1x radius accounting username-delimiter

To set the delimiter type, use `wireless security dot1x radius accounting username-delimiter` command, to remove the configuration, use the `no` form of this command.

```
wireless security dot1x radius accounting username-delimiter  { colon | hyphen | none | single-hyphen }
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>colon</td>
<td>Sets the delimiter to colon.</td>
</tr>
<tr>
<td>hyphen</td>
<td>Sets the delimiter to hyphen.</td>
</tr>
<tr>
<td>none</td>
<td>Disables delimiters.</td>
</tr>
<tr>
<td>single-hyphen</td>
<td>Sets the delimiters to single hyphen.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Command Modes</th>
<th>Global Configuration Mode.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cisco IOS XE 3.7.2 E</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

This example shows how to set the delimiter to colon.

```
Device(config)# wireless security dot1x radius accounting username-delimiter colon
```
wireless security dot1x radius callStationIdCase

To configure Call Station Id CASE send in RADIUS messages, use the `wireless security dot1x radius callStationIdCase` command.

To remove the Call Station Id CASE send in RADIUS messages, use the `no` form of the command.

`wireless security dot1x radius callStationIdCase { lower | upper }`

**Syntax Description**
- `lower` Sends all Call Station Ids to RADIUS in lowercase
- `upper` Sends all Call Station Ids to RADIUS in uppercase

**Command Default**
None

**Command Modes**
Global Configuration Mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.6.0 E</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

This example shows how to configure Call Station Id CASE send in RADIUS messages in lowercase:

```
Device(config)# wireless security dot1x radius callstationIdCase lower
```
wireless security dot1x radius mac-authentication call-station-id

To configure call station ID type for mac-authentication, use the `wireless security dot1x radius mac-authentication call-station-id` command. To remove the configuration, use the `no` form of it.

```
wireless security dot1x radius mac-authentication call-station-id ap-ethmac-only | ap-ethmac-ssid | ap-group-name | ap-label-address | ap-label-address-ssid | ap-location | ap-macaddress | ap-macaddress-ssid | ap-name | ap-name-ssid | ipaddress | macaddress | vlan-id
```

**Syntax Description**

- `ap-ethmac-only`: Sets call station ID type to the AP Ethernet MAC address.
- `ap-ethmac-ssid`: Sets call station ID type to the format 'AP Ethernet MAC address':'SSID'.
- `ap-group-name`: Sets call station ID type to the AP Group Name.
- `ap-label-address`: Sets call station ID type to the AP MAC address on AP Label.
- `ap-label-address-ssid`: Sets call station ID type to the format 'AP Label MAC address': 'SSID'.
- `ap-location`: Sets call station ID type to the AP Location.
- `ap-macaddress`: Sets call station ID type to the AP Radio MAC Address.
- `ap-macaddress-ssid`: Sets call station ID type to the 'AP radio MAC Address':'SSID'.
- `ap-name`: Sets call station ID type to the AP name.
- `ap-name-ssid`: Sets call station ID type to the format 'AP name': 'SSID'.
- `ipaddress`: Sets call station ID type to the system IP Address.
- `macaddress`: Sets call station ID type to the system MAC Address.
- `vlan-id`: Sets call station ID type to the VLAN ID.

**Command Default**

None

**Command Modes**

Global Configuration Mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.7.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>E</td>
<td></td>
</tr>
</tbody>
</table>

The example show how to set call station ID type to the AP Ethernet MAC address:

```
Device(config)# wireless security dot1x radius mac-authentication call-station-id ap-ethmac-only
```
To configure MAC-Authentication attributes, use the `wireless security dot1x radius mac-authentication mac-delimiter` command.

To remove MAC-Authentication attributes, use the `no` form of the command.

```
wireless security dot1x radius mac-authentication mac-delimiter { colon | hyphen | none | single-hyphen }
```

### Syntax Description

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>colon</td>
<td>Sets the delimiter to colon.</td>
</tr>
<tr>
<td>hyphen</td>
<td>Sets the delimiter to hyphen.</td>
</tr>
<tr>
<td>none</td>
<td>Disables delimiters.</td>
</tr>
<tr>
<td>single-hyphen</td>
<td>Sets the delimiters to single hyphen.</td>
</tr>
</tbody>
</table>

### Command Default

None

### Command Modes

Global Configuration Mode

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.6.0 E</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

This example shows how to configure MAC-Authentication attributes to colon:

```
Device(config)# Scurity dot1x radius mac-authentication mac-delimiter colon
```
wireless security web-auth retries

To enable web authentication retry on a particular WLAN, use the `wireless security web-auth retries` command. To disable, use the `no` form of the command.

`wireless securityweb-authretries retries`  
`nowireless securityweb-authretries`

**Syntax Description**

<table>
<thead>
<tr>
<th><code>wireless security web-auth</code></th>
<th>Enables web authentication on a particular WLAN.</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>retries retries</code></td>
<td>Specifies maximum number of web authentication request retries. The range is from 0 through 30. The default value is 3.</td>
</tr>
</tbody>
</table>

**Command Default**

`config`

**Command Modes**

`config`

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

None.

This example shows how to enable web authentication retry on a particular WLAN.

```
Device# configure terminal
Device# wireless security web-auth retries 10
```
wireless tag policy

To configure wireless tag policy, use the `wireless tag policy` command.

```
wireless tag policy policy-tag
```

**Syntax Description**

- `policy-tag`  Name of the wireless tag policy.

**Command Default**

The default policy tag is `default-policy-tag`.

**Command Modes**

Global configuration (config)

**Command History**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure a wireless policy tag:

```
Device(config)# wireless tag policy guest-policy
```
**wireless tag site**

To configure a wireless site tag, use the `wireless tag site site-tag` command.

```
wireless tag site site-tag
```

**Syntax Description**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>site-tag</strong></td>
<td>Name of the site tag.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

Global configuration (config)

**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>

**Example**

The following example shows how to configure a site tag:

```
Device(config)# wireless tag site test-site
```
wireless wps ap-authentication

To configure the access point neighbor authentication, use the `wireless wps ap-authentication` command. To remove the access point neighbor authentication, use the `no wireless wps ap-authentication` command.

```
wireless wps ap-authentication [threshold value]  
no wireless wps ap-authentication [threshold]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th><code>threshold value</code></th>
<th>Specifies that the WMM-enabled clients are on the wireless LAN. Threshold value (1 to 255).</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Command Modes</th>
<th><code>config</code></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th><code>Release</code></th>
<th><code>Modification</code></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cisco IOS XE</td>
<td>This command was</td>
</tr>
<tr>
<td></td>
<td>3.2SE</td>
<td>introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Usage Guidelines</th>
<th>None.</th>
</tr>
</thead>
</table>

This example shows how to set the threshold value for WMM-enabled clients.

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless wps ap-authentication threshold 65
```
wireless wps client-exclusion

To configure client exclusion policies, use the `wireless wps client-exclusion` command. To remove the client exclusion policies, use the `no` form of the command.

```
wireless wps client-exclusion {all|dot11-assoc|dot11-auth|dot1x-auth|dot1x-timeout|ip-theft|web-auth}
no wireless wps client-exclusion
{all|dot11-assoc|dot11-auth|dot1x-auth|dot1x-timeout|ip-theft|web-auth}
```

### Syntax Description

- **dot11-assoc**: Specifies that the controller excludes clients on the sixth 802.11 association attempt, after five consecutive failures.
- **dot11-auth**: Specifies that the controller excludes clients on the sixth 802.11 authentication attempt, after five consecutive failures.
- **dot1x-auth**: Specifies that the controller excludes clients on the sixth 802.11X authentication attempt, after five consecutive failures.
- **dot1x-timeout**: Enables exclusion on timeout and no response.
- **ip-theft**: Specifies that the controller excludes clients if the IP address is already assigned to another device.
  
  For more information, see the Usage Guidelines section.
- **web-auth**: Specifies that the controller excludes clients on the fourth web authentication attempt, after three consecutive failures.
- **all**: Specifies that the controller excludes clients for all of the above reasons.

### Command Default

Enabled.

### Command Modes

config

### Command History

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

### Usage Guidelines

In IP-theft scenarios, there are differences between the older Cisco IOS XE releases and the Cisco IOS XE Denali 16.x releases:
Older Cisco IOS XE Releases

Priority wise, wired clients have higher priority over wireless clients, and DHCP IP has higher priority over static IP. The client security type is not checked; security of all client types are treated with same priority.

If the existing binding is from a higher priority source, the new binding is ignored and an IP-theft is signaled. If the existing binding has the same source-priority as the new binding, the binding is ignored and an IP-theft is signaled. This ensures that the bindings are not toggled if two hosts send traffic using the same IP. Only the initial binding is retained in the software. If the new binding is from a higher priority source, the existing binding is replaced. This results in an IP-theft notification of existing binding and also a new binding notification.

There is not really a fundamental difference between wired and wireless; what matters is the trust (preflevel) of the entry, which is a function on how it was learnt (ARP, DHCP, ND, and so on) and the policy that is attached to the port. When preflevel is equal, the IP takeover is denied if the old entry is still reachable. IP takeover occurs when the update comes from a trusted port or a new entry gets IP from the DHCP server. Otherwise, you must explicitly grant it. The IP-theft is not reported if an old entry is replaced by a new and a more trusted one.

Cisco IOS XE Denali 16.x Releases

This example shows how to disable clients on the 802.11 association attempt after five consecutive failures.

Device#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)#wireless wps client-exclusion dot11-assoc

Device#
wireless wps rogue

To configure various rogue parameters, use the wireless wps rogue command.

wireless wps rogue {adhoc|client} [{alert mac-addr|contain mac-addr no-of-aps}]

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>adhoc</td>
<td>Configures the status of an Independent Basic Service Set (IBSS or ad-hoc) rogue access point.</td>
</tr>
<tr>
<td>client</td>
<td>Configures rogue clients</td>
</tr>
<tr>
<td>alert mac-addr</td>
<td>Generates an SNMP trap upon detection of the ad-hoc rogue, and generates an immediate alert to the system administrator for further action for the MAC address of the ad-hoc rogue access point.</td>
</tr>
<tr>
<td>contain mac-addr</td>
<td>Contains the offending device so that its signals no longer interfere with authorized clients.</td>
</tr>
<tr>
<td>no-of-aps</td>
<td>Maximum number of Cisco access points assigned to actively contain the ad-hoc rogue access point (1 through 4, inclusive).</td>
</tr>
</tbody>
</table>

**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 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

None.

This example shows how to generate an immediate alert to the system administrator for further action for the MAC address of the ad-hoc rogue access point.

```
Device#configure terminal
Enter configuration commands, one per line. End with CTRL/Z.
Device(config)#wireless wps rogue adhoc alert mac_addr
```
wireless wps rogue ap rldp alarm-only

To configure an alarm when a rogue is detected, use `wireless wps rogue ap rldp alarm-only` command. Use the `no` form of the command to disable the alarm.

```plaintext
[no] wireless wps rogue ap rldp alarm-only monitor-ap-only
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>monitor-ap-only</code></td>
<td>Perform RLDP only on monitor AP</td>
</tr>
</tbody>
</table>

### 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 3.2SE</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE 3.7.3E</td>
<td>The <code>no</code> form of the command was introduced.</td>
</tr>
</tbody>
</table>

### Example

This example shows how to configure an alarm for a detected rogue.

```plaintext
Device wireless wps rogue ap rldp alarm-only
```
wireless wps rogue ap rldp auto-contain

To configure RLDP, alarm and auto-contain if rogue is detected, use `wireless wps rogue ap rldp auto-contain` command. Use the `no` form of the command to disable the alarm.

```
[no] wireless wps rogue ap rldp auto-contain monitor-ap-only
```

**Syntax Description**

- `monitor-ap-only` Perform RLDP only on monitor AP

**Command Default**

None

**Command Modes**

Global Configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE 3.7.3E</td>
<td>The <code>no</code> form of the command was introduced.</td>
</tr>
</tbody>
</table>

**Example**

This example shows how to configure an alarm for a detected rogue.

```
Device wireless wps rogue ap rldp auto-contain
```
wireless wps rogue client

To configure the AAA server or MSE to validate if rogue clients are valid clients, use the wireless wps rogue client command.

wireless wps rogue client {aaa|mse}

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>Configures AAA or local database to detect valid MAC addresses.</td>
</tr>
<tr>
<td>mse</td>
<td>Configures MSE to detect valid MAC addresses.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>Global Configuration</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cisco IOS XE 3E</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

None

The following example shows how to configure AAA to detect valid MAC addresses.

Device wireless wps rogue client aaa

The following example shows how to configure MSE to detect valid MAC addresses.

Device wireless wps rogue client mse

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
wireless wps rogue detection

To configure various rogue detection parameters, use the `wireless wps rogue detection` command.

```
wireless wps rogue detection [{min-rssi rssi | min-transient-time transtime}]
```

**Syntax Description**

| min-rssi rssi | Configures the minimum RSSI value that rogues should have for APs to detect and for rogue entry to be created in the device. |
| min-transient-time transtime | Configures the time interval at which rogues have to be consistently scanned for by APs after the first time the rogues are scanned. |

**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 3.3SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

None.

This example shows how to configure rogue detection minimum RSSI value and minimum transient time:

```
Device# configure terminal
Device(config)# wireless wps rogue detection min-rssi 100
Device(config)# wireless wps rogue detection min-transient-time 500
Device(config)# end
```
wireless wps rogue rule

To configure rogue classification rule, use the **wireless wps rogue rule** command.

**wireless wps rogue rule** *rule-name* *priority* *priority*  
*classify* {friendly|malicious}  
*condition*  
{client-count number|duration|encryption|infrastructure|rssi|ssid}  
| default | exit | match {all|any} | no | shutdown |

**Syntax Description**

- **rule rule-name**: Specifies a rule name.
- **priority priority**: Changes the priority of a specific rule and shifts others in the list accordingly.
- **classify**: Specifies the classification of a rule.
- **friendly**: Classifies a rule as friendly.
- **malicious**: Classifies a rule as malicious.
- **condition**:  
  - **client-count number**: Requires that a minimum number of clients be associated to a rogue access point. The valid range is 1 to 10 (inclusive).
  - **duration**: Requires that a rogue access point be detected for a minimum period of time. The valid range is 0 to 3600 seconds (inclusive).
  - **encryption**: Requires that the advertised WLAN does not have encryption enabled.
  - **infrastructure**: Requires the SSID to be known to the controller.
  - **rssi**: Requires that a rogue access point have a minimum RSSI value. The range is from –95 to –50 dBm (inclusive).
  - **ssid**: Requires that a rogue access point have a specific SSID.

- **default**: Sets the command to its default settings.
- **exit**: Exits the sub-mode.
- **match {all | any}**: Configures matching criteria for a rule. Specifies whether a detected rogue access point must meet all or any of the conditions specified by the rule in order for the rule to be matched and the rogue access point to adopt the classification type of the rule.
- **no** : Negates a command or set its defaults.
- **shutdown** : Shuts down the system.

**Command Default**

None.

**Command Modes**

Global configuration
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.3SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

None.

This example shows how to create a rule that can organize and display rogue access points as Friendly:

```
Device# configure terminal
Device(config)# wireless wps rogue rule ap1 priority 1
Device(config-rule)# classify friendly
Device(config)# end
```
wireless-default radius server

To configure multiple radius servers, use the wireless-default radius server command.

wireless-default radius server IP key secret

Command Default
None

Command Modes
Global configuration (config)

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

Usage Guidelines
Using this utility, you can configure a maximum of ten radius servers.

Example
This example shows how to configure multiple radius servers:

Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless-default radius server 9.2.58.90 key cisco123
Device(config)# end
**wlan policy**

To map a policy profile to a WLAN profile, use the `wlan policy` command.

```
wlan wlan-name policy policy-name
```

**Syntax Description**

- `wlan-name` Name of the WLAN profile.
- `policy` Map a policy profile to the WLAN profile.
- `policy-name` Name of the policy profile.

**Command Default**

None

**Command Modes**

config-policy-tag

**Command History**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to map a policy to a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless tag policy demo-tag
Device(config-wireless-fabric)# wlan wlan1 policy policy1
```
Show Commands

- show access-list, on page 572
- show ap airtime-fairness summary, on page 574
- show ap auth-list, on page 575
- show ap auto-rf, on page 576
- show ap config, on page 578
- show ap crash-file, on page 579
- show ap dot11, on page 580
- show ap dot11, on page 586
- show ap dot11 24ghz , on page 587
- show ap dot11 24ghz SI config, on page 589
- show ap dot11 24ghz SI device type, on page 590
- show ap dot11 5ghz, on page 591
- show ap dot11 cleanair air-quality, on page 593
- show ap dot11 cleanair config, on page 594
- show ap dot11 cleanair summary, on page 596
- show ap environment, on page 597
- show ap filters active, on page 598
- show ap filters all, on page 599
- show ap fra, on page 600
- show ap gps location, on page 601
- show ap group hyperlocation, on page 602
- show ap hyperlocation, on page 604
- show ap hyperlocation cmx summary, on page 606
- show ap image, on page 607
- show ap link-encryption, on page 608
- show ap master list, on page 609
- show ap monitor-mode summary, on page 610
- show ap name auto-rf, on page 611
- show ap name cablemodem, on page 614
- show ap name config, on page 615
- show ap name config ethernet, on page 617
- show ap name dot11, on page 618
- show ap name environment, on page 621
• show ap name gps location, on page 622
• show ap name hyperlocation, on page 623
• show ap name mesh backhaul, on page 624
• show ap name mesh bhrate, on page 625
• show ap name mesh linktest, on page 626
• show ap name mesh neighbor detail, on page 627
• show ap name mesh path, on page 628
• show ap name mesh stats, on page 629
• show ap name wlan, on page 630
• show ap profile, on page 632
• show ap rf-profile name, on page 633
• show ap rf-profile summary, on page 635
• show ap summary, on page 636
• show ap tag sources, on page 637
• show ap tag summary, on page 638
• show ap upgrade, on page 639
• show arp, on page 640
• show arp summary, on page 641
• show avc client, on page 642
• show avc wlan, on page 643
• show chassis, on page 644
• show checkpoint, on page 645
• show etherchannel summary, on page 652
• show flow exporter, on page 653
• show flow interface, on page 655
• show flow monitor, on page 657
• show flow record, on page 659
• show interfaces, on page 660
• show ip, on page 664
• show ip device tracking, on page 665
• show ip igmp snooping igmpv2-tracking, on page 667
• show ip igmp snooping querier, on page 668
• show ip igmp snooping wireless mcast-spi-count, on page 670
• show ip igmp snooping wireless mgid, on page 671
• show ip nbar protocol-discovery wlan, on page 672
• show ipv6 access-list, on page 673
• show ipv6 mld snooping, on page 676
• show ipv6 mld snooping querier vlan, on page 678
• show ipv6 mld snooping wireless mgid, on page 679
• show ldap attributes, on page 680
• show ldap server, on page 681
• show lisp site detail, on page 682
• show logging profile wireless end timestamp, on page 683
• show logging profile wireless filter, on page 684
• show logging profile wireless fru, on page 685
• show logging profile wireless internal, on page 686
- show logging profile wireless level, on page 687
- show logging profile wireless module, on page 688
- show logging profile wireless reverse, on page 689
- show logging profile wireless start, on page 690
- show logging profile wireless switch, on page 691
- show logging profile wireless to-file, on page 692
- show mac access-group, on page 693
- show mobility, on page 694
- show nmsp, on page 696
- show nmsp cloud-services statistics, on page 697
- show nmsp cloud-services summary, on page 698
- show nmsp subscription group detail ap-list, on page 699
- show nmsp subscription group detail services, on page 700
- show nmsp subscription group summary, on page 701
- show platform conditions, on page 702
- show platform hardware, on page 703
- show platform hardware chassis active qfp feature dns-snoop-agent client enabled-intf, on page 704
- show platform hardware chassis active qfp feature dns-snoop-agent client hw-pattern-list, on page 705
- show platform hardware chassis active qfp feature dns-snoop-agent client info, on page 706
- show platform hardware chassis active qfp feature dns-snoop-agent client pattern-list, on page 707
- show platform hardware chassis active qfp feature dns-snoop-agent datapath ip-cache, on page 708
- show platform hardware chassis active qfp feature dns-snoop-agent datapath memory, on page 709
- show platform hardware chassis active qfp feature dns-snoop-agent datapath regexp-table, on page 710
- show platform hardware chassis active qfp feature dns-snoop-agent datapath stats, on page 711
- show platform hardware chassis active qfp feature et-analytics datapath runtime, on page 712
- show platform hardware chassis active qfp feature et-analytics datapath memory, on page 713
- show platform hardware chassis active qfp feature et-analytics datapath stats export, on page 714
- show platform hardware chassis active qfp feature et-analytics datapath stats flow, on page 715
- show platform hardware chassis active qfp feature wireless et-analytics eta-pending-client-tree, on page 716
- show platform hardware chassis active qfp feature wireless et-analytics statistics, on page 717
- show platform software trace filter-binary, on page 718
- show platform software trace filter-binary, on page 719
- show platform software trace level, on page 720
- show platform software trace message, on page 723
- show platform software trace message license-manager RP, on page 727
- show platform software trace message license-manager , on page 730
- show platform software utd chassis active F0 et-analytics global, on page 733
- show platform software et-analytics global, on page 734
- show parameter-map type umbrella global, on page 735
- show policy-map, on page 736
- show redundancy, on page 741
- show remote-lan all, on page 745
- show remote-lan id, on page 746
- show remote-lan name, on page 747
- show remote-lan policy detail, on page 748
• show remote-lan policy summary, on page 750
• show remote-lan summary, on page 751
• show ssh, on page 752
• show tech wireless client, on page 753
• show tech-support wireless, on page 757
• show tech-support wireless ap, on page 759
• show tech-support wireless client, on page 769
• show tech-support wireless datapath, on page 773
• show tech-support wireless fabric, on page 794
• show tech-support wireless mobility, on page 795
• show tech-support wireless radio, on page 807
• show umbrella config, on page 818
• show umbrella deviceid, on page 819
• show umbrella deviceid detailed, on page 820
• show umbrella dnsencrypt, on page 821
• show vlan, on page 822
• show vlan access-map, on page 825
• show vlan filter, on page 826
• show vlan group, on page 827
• show wireless band-select, on page 828
• show wireless client, on page 829
• show wireless client mac-address, on page 830
• show wireless client mac-address (Call Control), on page 831
• show wireless client mac-address (TCLAS), on page 832
• show wireless client mac-address mobility history, on page 833
• show wireless client summary, on page 834
• show wireless client timers, on page 835
• show wireless country, on page 836
• show wireless detail, on page 839
• show wireless dot11h, on page 840
• show wireless dtls connections, on page 841
• show wireless exclusionlist, on page 842
• show wireless fabric summary, on page 843
• show wireless fabric client summary, on page 844
• show wireless fabric v nid mapping, on page 845
• show wireless flow-control, on page 846
• show wireless flow-control statistics, on page 847
• show wireless load-balancing, on page 848
• show wireless media-stream client detail, on page 849
• show wireless media-stream group, on page 850
• show wireless media-stream message details, on page 851
• show wireless mobility controller ap, on page 852
• show wireless media-stream multicast-direct state, on page 853
• show wireless mesh ap, on page 854
• show wireless mesh ap summary, on page 855
• show wireless mesh ap tree, on page 856
show access-list

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

```
show access-lists [number|name|hardware counters|ipc]
```

**Syntax Description**

- **number** (Optional) ACL number. The range is 1 to 2799.
- **name** (Optional) Name of the ACL.
- **hardware counters** (Optional) Displays global hardware ACL statistics for switched and routed packets.
- **ipc** (Optional) Display Interprocess Communication (IPC) protocol access-list configuration download information.

**Command Default**

Privileged EXEC

**Command Modes**

- **EXEC**

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>3.2SE</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

The switch 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
Extended MAC access list mac1
```

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
```
### L3 ACL OUTPUT Statistics

<table>
<thead>
<tr>
<th>Action Description</th>
<th>Frame Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Drop</td>
<td>0</td>
</tr>
<tr>
<td>All Bridge Only</td>
<td>0</td>
</tr>
<tr>
<td>All Forwarding To CPU</td>
<td>0</td>
</tr>
<tr>
<td>All Forwarded</td>
<td>266050</td>
</tr>
<tr>
<td>All Drop And Log</td>
<td>0</td>
</tr>
<tr>
<td>All Bridge Only And Log</td>
<td>0</td>
</tr>
<tr>
<td>All Forwarded And Log</td>
<td>0</td>
</tr>
<tr>
<td>All IPv6 Drop</td>
<td>0</td>
</tr>
<tr>
<td>All IPv6 Bridge Only</td>
<td>0</td>
</tr>
<tr>
<td>All IPv6 Forwarding To CPU</td>
<td>0</td>
</tr>
<tr>
<td>All IPv6 Forwarded</td>
<td>0</td>
</tr>
<tr>
<td>All IPv6 Drop And Log</td>
<td>0</td>
</tr>
<tr>
<td>All IPv6 Bridge Only And Log</td>
<td>0</td>
</tr>
<tr>
<td>All IPv6 Forwarded And Log</td>
<td>0</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list</td>
<td>Enables smart logging for a standard or extended IP access list.</td>
</tr>
</tbody>
</table>
**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**

<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>

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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>chassis-number</code> Chassis number as either 1 or 2.</td>
</tr>
<tr>
<td><code>active R0</code>     Active instance in Route-processor slot 0.</td>
</tr>
<tr>
<td><code>standby R0</code>    Standby instance in Route-processor slot 0.</td>
</tr>
</tbody>
</table>

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

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

```
Device# show ap auth-list
```
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 802.11 {a | b} cisco_ap
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>a</strong></td>
<td>Specifies the 802.11a network.</td>
</tr>
<tr>
<td><strong>b</strong></td>
<td>Specifies the 802.11b/g network.</td>
</tr>
<tr>
<td><strong>cisco_ap</strong></td>
<td>Cisco lightweight access point name.</td>
</tr>
</tbody>
</table>

**Command Default**

None

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

```plaintext
(Cisco Controller) > show ap auto-rf 802.11a AP1
Number Of Slots............................... 2
AP Name........................................ AP03
MAC Address.................................... 00:0b:85:01:18:b7
Radio Type..................................... RADIO_TYPE_80211a
Noise Information
  Noise Profile............................... PASSED
  Channel 36.................................. -88 dBm
  Channel 40.................................. -86 dBm
  Channel 44.................................. -87 dBm
  Channel 48.................................. -85 dBm
  Channel 52.................................. -84 dBm
  Channel 56.................................. -83 dBm
  Channel 60.................................. -84 dBm
  Channel 64.................................. -85 dBm
Interference Information
  Interference Profile......................... PASSED
  Channel 36.................................. -66 dBm @ 1% busy
  Channel 40.................................. -128 dBm @ 0% busy
  Channel 44.................................. -128 dBm @ 0% busy
  Channel 48.................................. -128 dBm @ 0% busy
  Channel 52.................................. -128 dBm @ 0% busy
  Channel 56.................................. -73 dBm @ 1% busy
  Channel 60.................................. -55 dBm @ 1% busy
  Channel 64.................................. -69 dBm @ 1% busy
Rogue Histogram (20/40_ABOVE/40_BELOW)
  Channel 36.................................. 16/ 0/ 0
  Channel 40.................................. 28/ 0/ 0
  Channel 44.................................. 9/ 0/ 0
  Channel 48.................................. 9/ 0/ 0
  Channel 52.................................. 3/ 0/ 0
  Channel 56.................................. 4/ 0/ 0
  Channel 60.................................. 7/ 1/ 0
  Channel 64.................................. 2/ 0/ 0
```
Load Information
Load Profile........................................ PASSED
Receive Utilization................................. 0%
Transmit Utilization................................. 0%
Channel Utilization................................. 1%
Attached Clients................................. 1 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 dBm........................................ 0 clients
SNR 5 dBm........................................ 0 clients
SNR 10 dBm......................................... 0 clients
SNR 15 dBm......................................... 0 clients
SNR 20 dBm......................................... 0 clients
SNR 25 dBm......................................... 0 clients
SNR 30 dBm......................................... 0 clients
SNR 35 dBm......................................... 0 clients
SNR 40 dBm......................................... 0 clients
SNR 45 dBm......................................... 0 clients

Nearby RADs
RAD 00:0b:85:01:05:08 slot 0................. -46 dBm on 10.1.30.170
RAD 00:0b:85:01:12:65 slot 0................. -24 dBm on 10.1.30.170

Channel Assignment Information
Current Channel Average Energy................. -86 dBm
Previous Channel Average Energy................ -75 dBm
Channel Change Count........................... 109
Last Channel Change Time....................... Wed Sep 29 12:53:34 2004

Recommended Best Channel.................... 44

RF Parameter Recommendations
Power Level....................................... 1
RTS/CTS Threshold............................... 2347
Fragmentation Threshold....................... 2346
Antenna Pattern.................................. 0
**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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ethernet</code></td>
<td>Displays ethernet VLAN tagging information for all Cisco APs.</td>
</tr>
<tr>
<td><code>general</code></td>
<td>Displays common information for all Cisco APs.</td>
</tr>
<tr>
<td><code>global</code></td>
<td>Displays global settings for all Cisco APs.</td>
</tr>
</tbody>
</table>

### Command Default

None

### Command Modes

Any command mode

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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 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
```

**Syntax Description**

This command has no keywords and arguments.

**Command Default**

None

**Command Modes**

Any command mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

```
Device# show ap crash-file
```
To view 802.11a or 802.11b configuration information, use the **show ap dot11** command.

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>24ghz</td>
<td>Specifies the 2.4 GHz band.</td>
</tr>
<tr>
<td>5ghz</td>
<td>Specifies the 5 GHz band.</td>
</tr>
<tr>
<td>channel</td>
<td>Displays the automatic channel assignment configuration and statistics.</td>
</tr>
<tr>
<td>coverage</td>
<td>Displays the configuration and statistics for coverage hole detection.</td>
</tr>
<tr>
<td>group</td>
<td>Displays 802.11a or 802.11b Cisco radio RF grouping.</td>
</tr>
<tr>
<td>load-info</td>
<td>Displays channel utilization and client count information for all Cisco APs.</td>
</tr>
<tr>
<td>logging</td>
<td>Displays 802.11a or 802.11b RF event and performance logging.</td>
</tr>
<tr>
<td>media-stream</td>
<td>Display 802.11a or 802.11b Media Resource Reservation Control configurations.</td>
</tr>
<tr>
<td>monitor</td>
<td>Displays the 802.11a or 802.11b default Cisco radio monitoring.</td>
</tr>
<tr>
<td>network</td>
<td>Displays the 802.11a or 802.11b network configuration.</td>
</tr>
<tr>
<td>profile</td>
<td>Displays the 802.11a or 802.11b lightweight access point performance profiles.</td>
</tr>
<tr>
<td>receiver</td>
<td>Displays the configuration and statistics of the 802.11a or 802.11b receiver.</td>
</tr>
<tr>
<td>service-policy</td>
<td>Displays the Quality of Service (QoS) service policies for 802.11a or 802.11b radio for all Cisco access points.</td>
</tr>
<tr>
<td>summary</td>
<td>Displays the 802.11a or 802.11b Cisco lightweight access point name, channel, and transmit level summary.</td>
</tr>
<tr>
<td>txpower</td>
<td>Displays the 802.11a or 802.11b automatic transmit power assignment.</td>
</tr>
<tr>
<td>ccx global</td>
<td>Displays 802.11a or 802.11b Cisco Client eXtensions (CCX) information for all Cisco access points that are joined to the device.</td>
</tr>
</tbody>
</table>
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          : 36,40,44,48,52,56,60,64,149,153,157,161
  802.11a 4.9 GHz Auto-RF Channel List
    Allowed Channel List          : 1,2,3,4,5,6,7,8,9,10,11,12,13,14,
    Unused Channel List           : 1,2,3,4,5,6,7,8,9,10,11,12,13,14,
  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 lever........ 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}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>media-stream rrc</code></td>
<td>Displays Media Stream configurations.</td>
</tr>
<tr>
<td><code>network</code></td>
<td>Shows network configuration.</td>
</tr>
<tr>
<td><code>profile</code></td>
<td>Shows profiling information for all Cisco APs.</td>
</tr>
<tr>
<td><code>summary</code></td>
<td>Shows configuration and statistics of 802.11b and 802.11a Cisco APs.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>User EXEC command mode or Privileged EXEC command mode</td>
</tr>
<tr>
<td>Usage Guidelines</td>
<td>None.</td>
</tr>
</tbody>
</table>

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**

- **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 L2 roam 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11b Global coverage exception level</td>
<td>25 %</td>
</tr>
<tr>
<td>802.11b Global client minimum exception level</td>
<td>3 clients</td>
</tr>
</tbody>
</table>
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**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**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.
- **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**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**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**

- `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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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, 157, 161


802.11a 4.9 GHz Auto-RF Channel List
- Allowed 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
- 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 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}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>24ghz</th>
<th>Displays the 2.4 GHz band.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>5ghz</td>
<td>Displays the 5 GHz band.</td>
</tr>
<tr>
<td>summary</td>
<td></td>
<td>Displays a summary of 802.11 radio band air-quality information.</td>
</tr>
<tr>
<td>worst</td>
<td></td>
<td>Displays the worst air-quality information for 802.11 networks.</td>
</tr>
</tbody>
</table>

**Command Default**
None

**Command Modes**
Any command mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>24ghz</th>
<th>Displays the 2.4 GHz band.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>5ghz</td>
<td>Displays the 5 GHz band.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>Any command mode</td>
</tr>
<tr>
<td>Command History</td>
<td>Release</td>
</tr>
<tr>
<td></td>
<td>Cisco IOS XE 3.2SE</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
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**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

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

```
Device# show ap environment
```
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**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**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 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**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**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 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**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

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

```
Device# show ap fra
```
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]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Chassis Number</th>
<th>Active Instance of the AP Filters in Route-Processor Slot 0</th>
<th>Standby Instance of the AP Filters in Route-Processor Slot 0</th>
</tr>
</thead>
<tbody>
<tr>
<td>chassis-number</td>
<td>Enter the chassis number as either 1 or 2.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>active R0</td>
<td>Active instance of the AP filters in Route-processor slot 0.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>standby R0</td>
<td>Standby instance of the AP filters in Route-processor slot 0.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

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

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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>summary</td>
<td>Shows the overall configuration values (AP group specific) and operational status and parameters for the AP group.</td>
</tr>
<tr>
<td>detail</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Command Modes**

- User EXEC
- Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Denali 16.3.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>AP Name</th>
<th>Radio MAC</th>
<th>Method</th>
<th>Hyperlocation</th>
</tr>
</thead>
<tbody>
<tr>
<td>APf07f.0635.2d40</td>
<td>f07f.0676.3b89</td>
<td>WSM</td>
<td>Enabled</td>
</tr>
<tr>
<td>APf4cf.e272.4ed0</td>
<td>f4cf.e223.ba31</td>
<td>Local</td>
<td>Enabled</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>summary</code></td>
<td>Shows the overall configuration and operational values.</td>
</tr>
<tr>
<td><code>detail</code></td>
<td>Shows the overall configuration and operation values as well as detailed information about each AP.</td>
</tr>
</tbody>
</table>

### Command Default

None

### Command History

- 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
```
<table>
<thead>
<tr>
<th>AP Name</th>
<th>Radio MAC</th>
<th>Method</th>
<th>Hyperlocation</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP84b8.0252.b930</td>
<td>84b8.0216.c721</td>
<td>HALO</td>
<td>Enabled</td>
</tr>
<tr>
<td>AP84b8.0265.5540</td>
<td>84b8.0243.8796</td>
<td>MSM</td>
<td>Enabled</td>
</tr>
<tr>
<td>APf07f.0635.2d40</td>
<td>f07f.0676.3b89</td>
<td>MSM</td>
<td>Enabled</td>
</tr>
<tr>
<td>APf4cf.e272.4ed0</td>
<td>f4cf.e223.ba31</td>
<td>HALO</td>
<td>Enabled</td>
</tr>
</tbody>
</table>
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**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

```
Device# show ap image
```
show ap link-encryption

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

```
show ap link-encryption
```

**Syntax Description**

This command has no keywords and arguments.

**Command Default**

None

**Command Modes**

Any command mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

```
Device# show ap link-encryption
```
show ap master list

To see the AP master list, use the `show ap master list` command.

```
show ap master {chassis | {chassis-number | active | standby} | R0} list
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>chassis-number</code></td>
<td>Chassis number as either 1 or 2.</td>
</tr>
<tr>
<td><code>active R0</code></td>
<td>Active instance in Route-processor slot 0.</td>
</tr>
<tr>
<td><code>standby R0</code></td>
<td>Standby instance in Route-processor slot 0.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
</table>
| 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 master list:

```
Device# show ap master list
```
**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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 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}
```

**Syntax Description**

- **ap-name**: Name of the Cisco lightweight access point.
- **24ghz**: Displays the 2.4 GHz band.
- **5ghz**: Displays the 5 GHz band.

**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 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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
  - **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
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 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**

- **ap-name**: Name of the AP.
- **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**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**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}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ap-name</td>
<td>Name of the Cisco lightweight access point.</td>
</tr>
<tr>
<td>ethernet</td>
<td>Displays Ethernet tagging configuration information for an access point.</td>
</tr>
<tr>
<td>general</td>
<td>Displays common information for an access point.</td>
</tr>
</tbody>
</table>

| Command Modes      | Any command mode |

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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: Te1/0/1
- 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
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tertiary Cisco Controller Name</td>
<td>:</td>
</tr>
<tr>
<td>Tertiary Cisco Controller IP Address</td>
<td>: Not Configured</td>
</tr>
<tr>
<td>Administrative State</td>
<td>: Enabled</td>
</tr>
<tr>
<td>Operation State</td>
<td>: Registered</td>
</tr>
<tr>
<td>AP Mode</td>
<td>: Local</td>
</tr>
<tr>
<td>AP Submode</td>
<td>: Not Configured</td>
</tr>
<tr>
<td>Remote AP Debug</td>
<td>: Disabled</td>
</tr>
<tr>
<td>Logging Trap Severity Level</td>
<td>: informational</td>
</tr>
<tr>
<td>Software Version</td>
<td>: 7.4.0.5</td>
</tr>
<tr>
<td>Boot Version</td>
<td>: 7.4.0.5</td>
</tr>
<tr>
<td>Stats Reporting Period</td>
<td>: 180</td>
</tr>
<tr>
<td>LED State</td>
<td>: Enabled</td>
</tr>
<tr>
<td>PoE Pre-Standard Switch</td>
<td>: Disabled</td>
</tr>
<tr>
<td>PoE Power Injector MAC Address</td>
<td>: Disabled</td>
</tr>
<tr>
<td>Power Type/Mode</td>
<td>: Power Injector/Normal Mode</td>
</tr>
<tr>
<td>Number of Slots</td>
<td>: 2</td>
</tr>
<tr>
<td>AP Model</td>
<td>: 1140AG</td>
</tr>
<tr>
<td>AP Image</td>
<td>: C1140-K0W8-M</td>
</tr>
<tr>
<td>IOS Version</td>
<td>:</td>
</tr>
<tr>
<td>Reset Button</td>
<td>:</td>
</tr>
<tr>
<td>AP Serial Number</td>
<td>: SIM1140K001</td>
</tr>
<tr>
<td>AP Certificate Type</td>
<td>: Manufacture Installed</td>
</tr>
<tr>
<td>Management Frame Protection Validation</td>
<td>: Disabled</td>
</tr>
<tr>
<td>AP User Mode</td>
<td>: Customized</td>
</tr>
<tr>
<td>AP User Name</td>
<td>: cisco</td>
</tr>
<tr>
<td>AP 802.1X User Mode</td>
<td>: Not Configured</td>
</tr>
<tr>
<td>AP 802.1X User Name</td>
<td>: Not Configured</td>
</tr>
<tr>
<td>Cisco AP System Logging Host</td>
<td>: 255.255.255.255</td>
</tr>
<tr>
<td>AP Up Time</td>
<td>: 15 days 16 hours 19 minutes 57 seconds</td>
</tr>
<tr>
<td>AP CAPWAP Up Time</td>
<td>: 4 minutes 56 seconds</td>
</tr>
<tr>
<td>Join Date and Time</td>
<td>: 10/18/2012 04:48:56</td>
</tr>
<tr>
<td>Join Taken Time</td>
<td>: 15 days 16 hours 15 minutes 0 seconds</td>
</tr>
<tr>
<td>Join Priority</td>
<td>: 1</td>
</tr>
<tr>
<td>Ethernet Port Duplex</td>
<td>: Auto</td>
</tr>
<tr>
<td>Ethernet Port Speed</td>
<td>: Auto</td>
</tr>
<tr>
<td>AP Link Latency</td>
<td>: Disabled</td>
</tr>
<tr>
<td>Rogue Detection</td>
<td>: Disabled</td>
</tr>
<tr>
<td>AP TCP MSS Adjust</td>
<td>: Disabled</td>
</tr>
<tr>
<td>AP TCP MSS Size</td>
<td>: 6146</td>
</tr>
</tbody>
</table>
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**

- `ap-name` Name of the AP.
- `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**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**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} {ccx|cdp|profile|service-policy output|stats|tsm {all|client-mac}}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ap-name</code></td>
<td>Name of the Cisco lightweight access point.</td>
</tr>
<tr>
<td><code>24ghz</code></td>
<td>Displays the 2.4 GHz band.</td>
</tr>
<tr>
<td><code>5ghz</code></td>
<td>Displays the 5 GHz band.</td>
</tr>
<tr>
<td><code>ccx</code></td>
<td>Displays the Cisco ClienteXtensions (CCX) radio management status information.</td>
</tr>
<tr>
<td><code>cdp</code></td>
<td>Displays Cisco Discovery Protocol (CDP) information.</td>
</tr>
<tr>
<td><code>profile</code></td>
<td>Displays configuration and statistics of 802.11 profiling.</td>
</tr>
<tr>
<td><code>service-policy output</code></td>
<td>Displays downstream service policy information.</td>
</tr>
<tr>
<td><code>stats</code></td>
<td>Displays Cisco lightweight access point statistics.</td>
</tr>
<tr>
<td><code>tsm</code></td>
<td>Displays 802.11 traffic stream metrics statistics.</td>
</tr>
<tr>
<td><code>all</code></td>
<td>Displays the list of all access points to which the client has associations.</td>
</tr>
<tr>
<td><code>client-mac</code></td>
<td>MAC address of the client.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

Any command mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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 shows how to display CDP information for a specific access point:
show ap name AP01 dot11 24ghz cdp

<table>
<thead>
<tr>
<th>AP Name</th>
<th>AP CDP State</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP03</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

This example shows 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 shows 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 shows how to display statistics for a specific access point:

Device# show ap name AP01 dot11 24ghz stats

Number of Users.................................: 0
TxFragmentCount...............................: 0
MulticastTxFrameCnt..........................: 0
FailedCount....................................: 0
RetryCount.....................................: 0
MultipleRetryCount............................: 0
FrameDuplicateCount...........................: 0
RtsSuccessCount...............................: 0
RtsFailureCount...............................: 0
AckFailureCount...............................: 0
RxIncompleteFragment........................: 0
MulticastRxFrameCnt..........................: 0
FcsErrorCount..................................: 0
TxFrameCount...................................: 0
WepUndecryptableCount.......................: 0
TxFramesDropped................................: 0

Call Admission Control (CAC) Stats
Voice Bandwidth in use(% of config bw)........: 0
Video Bandwidth in use(% of config bw)........: 0
Total BW in use for Voice(%)...................: 0
Total BW in use for SIP Preferred call(%).....: 0

Load based Voice Call Stats
Total channel MT free..........................: 0
Total voice MT free............................: 0
Na Direct......................................: 0
Na Roam........................................: 0

WMM TSPEC CAC Call Stats
Total num of voice calls in progress...........: 0
Num of roaming voice calls in progress.........: 0
Total Num of voice calls since AP joined......: 0
Total Num of roaming calls since AP joined......: 0
Total Num of exp bw requests received........: 0
Total Num of exp bw requests admitted.......: 0
Num of voice calls rejected since AP joined.: 0
Num of roam calls rejected since AP joined:...: 0
Num of calls rejected due to insufficient bw.: 0
Num of calls rejected due to invalid params.: 0
Num of calls rejected due to PHY rate.......: 0
Num of calls rejected due to QoS policy.....: 0

SIP CAC Call Stats
Total Num of calls in progress..............: 0
Num of roaming calls in progress............: 0
Total Num of calls since AP joined.........: 0
Total Num of roaming calls since AP joined.: 0
Total Num of Preferred calls received......: 0
Total Num of Preferred calls accepted......: 0
Total Num of ongoing Preferred calls......: 0
Total Num of calls rejected(Insuff BW)...: 0
Total Num of roam calls rejected(Insuff BW): 0

Band Select Stats
Num of dual band client ..................: 0
Num of dual band client added.............: 0
Num of dual band client expired ..........: 0
Num of dual band client replaced.........: 0
Num of dual band client detected.........: 0
Num of suppressed client ...............: 0
Num of suppressed client expired........: 0
Num of suppressed client replaced.......: 0

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 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**

- `ap-name` Name of the AP.
- `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**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**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
```

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

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**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 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`

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ap-name</code></td>
<td></td>
<td>Access point name.</td>
</tr>
<tr>
<td><code>hyperlocation</code></td>
<td></td>
<td>Displays AP hyperlocation information.</td>
</tr>
<tr>
<td><code>ble-beacon</code></td>
<td></td>
<td>Displays BLE beacon configuration of an AP.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Denali 16.3.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Example**

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

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

<table>
<thead>
<tr>
<th>ID</th>
<th>Major</th>
<th>Minor</th>
<th>TX Power(dBm)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```
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**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**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 bachkhaul 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]
```

<table>
<thead>
<tr>
<th>ap-name</th>
<th>Name of the AP.</th>
</tr>
</thead>
<tbody>
<tr>
<td>chassis-number</td>
<td>Enter the chassis number as either 1 or 2.</td>
</tr>
<tr>
<td>active R0</td>
<td>Active instance of the AP filters in Route-processor slot 0.</td>
</tr>
<tr>
<td>standby R0</td>
<td>Standby instance of the AP filters in Route-processor slot 0.</td>
</tr>
</tbody>
</table>

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to see mesh bachkhaul 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]
```

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

**Command Default**

None

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th><strong>Release</strong></th>
<th><strong>Modification</strong></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>

**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**

- `ap-name` Name of the AP.
- `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**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**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**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ap-name</code></td>
<td>Name of the AP.</td>
</tr>
<tr>
<td><code>packet error</code></td>
<td>Mesh packet error statistics.</td>
</tr>
<tr>
<td><code>queue</code></td>
<td>Mesh queue statistics.</td>
</tr>
<tr>
<td><code>security</code></td>
<td>Mesh security statistics.</td>
</tr>
<tr>
<td><code>chassis-number</code></td>
<td>Enter the chassis number as either 1 or 2.</td>
</tr>
<tr>
<td><code>active R0</code></td>
<td>Active instance of the AP filters in Route-processor slot 0.</td>
</tr>
<tr>
<td><code>standby R0</code></td>
<td>Standby instance of the AP filters in Route-processor slot 0.</td>
</tr>
</tbody>
</table>

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to see mesh statistics:

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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ap-name</strong></td>
<td>Name of the Cisco lightweight access point.</td>
</tr>
<tr>
<td><strong>dot11</strong></td>
<td>Displays 802.11 parameters.</td>
</tr>
<tr>
<td><strong>24ghz</strong></td>
<td>Displays 802.11b network settings.</td>
</tr>
<tr>
<td><strong>5ghz</strong></td>
<td>Displays 802.11a network settings.</td>
</tr>
<tr>
<td><strong>statistic</strong></td>
<td>Displays WLAN statistics.</td>
</tr>
</tbody>
</table>

**Command Default:** None

**Command Modes:** Any command mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

```plaintext
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:

```plaintext
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
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>EAP Id Request Msg Timeouts</td>
<td>0</td>
</tr>
<tr>
<td>EAP Id Request Msg Timeouts Failures</td>
<td>0</td>
</tr>
<tr>
<td>EAP Request Msg Timeouts</td>
<td>0</td>
</tr>
<tr>
<td>EAP Request Msg Timeouts Failures</td>
<td>0</td>
</tr>
<tr>
<td>EAP Key Msg Timeouts</td>
<td>0</td>
</tr>
<tr>
<td>EAP Key Msg Timeouts Failures</td>
<td>0</td>
</tr>
</tbody>
</table>
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**

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

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>profile-name</strong></td>
<td>Name of the RF-Profile.</td>
</tr>
<tr>
<td><strong>detail</strong></td>
<td>Show detail of selected RF Profile.</td>
</tr>
</tbody>
</table>

**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 Denali 16.3.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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
```
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**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Command Default</th>
<th>Command Modes</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>summary</td>
<td>None</td>
<td>Privileged EXEC</td>
<td>Cisco IOS XE Denali 16.3.1 This command was introduced.</td>
</tr>
</tbody>
</table>

**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 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**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>This command has no keywords and arguments.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Default</td>
<td>None</td>
</tr>
<tr>
<td>Command Modes</td>
<td>Any command mode</td>
</tr>
<tr>
<td>Command History</td>
<td>Release</td>
</tr>
<tr>
<td></td>
<td>Cisco IOS XE 3.2SE</td>
</tr>
</tbody>
</table>

**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
```

<table>
<thead>
<tr>
<th>AP Name</th>
<th>AP Model</th>
<th>Ethernet MAC</th>
<th>Radio MAC</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>3602a</td>
<td>3502I</td>
<td>003.a.9eb.3fa8</td>
<td>d0c2.8267.8b00</td>
<td>Registered</td>
</tr>
</tbody>
</table>

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**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**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

<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>

Example

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

Device# show ap tag summary
**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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name ap-upgrade-report-name</td>
<td>Enter the name of the AP upgrade report.</td>
</tr>
<tr>
<td>summary</td>
<td>Shows a summary of AP upgrade information.</td>
</tr>
<tr>
<td>chassis-number</td>
<td>Enter the chassis number as either 1 or 2.</td>
</tr>
<tr>
<td>active R0</td>
<td>Active instance in Route-processor slot 0.</td>
</tr>
<tr>
<td>standby R0</td>
<td>Standby instance in Route-processor slot 0.</td>
</tr>
</tbody>
</table>

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to see a summary of the AP upgrade information:

```
Device# show ap upgrade summary
```
show arp

To view the ARP table, use the `show arp` command.

```
show arp
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>arp</code></td>
<td>Shows ARP table</td>
</tr>
</tbody>
</table>

**Command Modes**

- User EXEC (`>`)
- Privileged EXEC (`#`)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.111.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

The following example shows a sample output of the command:

```
cisco-wave2-ap# 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
```

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>Privileged EXEC</td>
</tr>
</tbody>
</table>

| 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 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.3SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

The following is sample output from the `show avc client` command:

```plaintext
Device# sh avc client 0040.96ae.65ec top 10 application aggregate

Cumulative Stats:

<table>
<thead>
<tr>
<th>No.</th>
<th>AppName</th>
<th>Packet-Count</th>
<th>Byte-Count</th>
<th>AvgPkt-Size</th>
<th>usage%</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>skinny</td>
<td>7343</td>
<td>449860</td>
<td>61</td>
<td>94</td>
</tr>
<tr>
<td>2</td>
<td>unknown</td>
<td>99</td>
<td>13631</td>
<td>137</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>dhcp</td>
<td>18</td>
<td>8752</td>
<td>486</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>http</td>
<td>18</td>
<td>3264</td>
<td>181</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>tftp</td>
<td>9</td>
<td>534</td>
<td>59</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>dns</td>
<td>2</td>
<td>224</td>
<td>112</td>
<td>0</td>
</tr>
</tbody>
</table>

Last Interval (90 seconds) Stats:

<table>
<thead>
<tr>
<th>No.</th>
<th>AppName</th>
<th>Packet-Count</th>
<th>Byte-Count</th>
<th>AvgPkt-Size</th>
<th>usage%</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>skinny</td>
<td>9</td>
<td>540</td>
<td>60</td>
<td>100</td>
</tr>
</tbody>
</table>
```
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**

- `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**

Cisco IOS XE 3.3SE  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:

<table>
<thead>
<tr>
<th>No.</th>
<th>AppName</th>
<th>Packet-Count</th>
<th>Byte-Count</th>
<th>AvgPkt-Size</th>
<th>usage%</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ssl</td>
<td>10598677</td>
<td>1979525706</td>
<td>997</td>
<td>42</td>
</tr>
<tr>
<td>2</td>
<td>vnc</td>
<td>5550900</td>
<td>376412847</td>
<td>678</td>
<td>14</td>
</tr>
<tr>
<td>3</td>
<td>http</td>
<td>3043131</td>
<td>2691327197</td>
<td>884</td>
<td>10</td>
</tr>
<tr>
<td>4</td>
<td>unknown</td>
<td>1856297</td>
<td>1140264956</td>
<td>614</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>video-over-http</td>
<td>1625019</td>
<td>2063335150</td>
<td>1269</td>
<td>8</td>
</tr>
<tr>
<td>6</td>
<td>binary-over-http</td>
<td>1329115</td>
<td>1744190344</td>
<td>1312</td>
<td>6</td>
</tr>
<tr>
<td>7</td>
<td>webex-meeting</td>
<td>1146872</td>
<td>540713787</td>
<td>471</td>
<td>2</td>
</tr>
<tr>
<td>8</td>
<td>rtp</td>
<td>923900</td>
<td>635650544</td>
<td>688</td>
<td>3</td>
</tr>
<tr>
<td>9</td>
<td>unknown</td>
<td>752341</td>
<td>911002213</td>
<td>1210</td>
<td>3</td>
</tr>
<tr>
<td>10</td>
<td>youtube</td>
<td>631085</td>
<td>706636186</td>
<td>1119</td>
<td>3</td>
</tr>
</tbody>
</table>

Last Interval(90 seconds) Stats:

```
<table>
<thead>
<tr>
<th>No.</th>
<th>AppName</th>
<th>Packet-Count</th>
<th>Byte-Count</th>
<th>AvgPkt-Size</th>
<th>usage%</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>vnc</td>
<td>687093</td>
<td>602731844</td>
<td>877</td>
<td>68</td>
</tr>
<tr>
<td>2</td>
<td>video-over-http</td>
<td>213272</td>
<td>279831588</td>
<td>1312</td>
<td>31</td>
</tr>
<tr>
<td>3</td>
<td>ssl</td>
<td>6515</td>
<td>5029365</td>
<td>771</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>webex-meeting</td>
<td>3649</td>
<td>1722663</td>
<td>472</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>http</td>
<td>2634</td>
<td>1334355</td>
<td>506</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>unknown</td>
<td>1436</td>
<td>99412</td>
<td>69</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>google-services</td>
<td>722</td>
<td>378121</td>
<td>523</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>linkedin</td>
<td>655</td>
<td>393263</td>
<td>600</td>
<td>0</td>
</tr>
<tr>
<td>9</td>
<td>exchange</td>
<td>432</td>
<td>167390</td>
<td>387</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>gtalk-chat</td>
<td>330</td>
<td>17330</td>
<td>52</td>
<td>0</td>
</tr>
</tbody>
</table>
```
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 switch.
  - `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 checkpoint

To display information about the Checkpoint Facility (CF) subsystem, use the show checkpoint command.

**show checkpoint clients entities statistics**

**Syntax Description**
- **clients**: Displays detailed information about checkpoint clients.
- **entities**: Displays detailed information about checkpoint entities.
- **statistics**: Displays detailed information about checkpoint statistics.

**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 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Client Name</th>
<th>Client Entity</th>
<th>Bundle Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network RF Client</td>
<td>3</td>
<td>--</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Client Name</th>
<th>Client ID</th>
<th>Entity ID</th>
<th>Bundle Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network RF Client</td>
<td>3</td>
<td>--</td>
<td>Off</td>
</tr>
<tr>
<td>SNMP CF Client</td>
<td>12</td>
<td>--</td>
<td>Off</td>
</tr>
<tr>
<td>------------------</td>
<td>--------</td>
<td>-----</td>
<td>-----</td>
</tr>
<tr>
<td>Total API Messages Sent:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total Transport Messages Sent:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Length of Sent Messages:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total Blocked Messages Sent:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Length of Sent Blocked Messages:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total Non-blocked Messages Sent:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Length of Sent Non-blocked Messages:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total Bytes Allocated:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Buffers Held:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Buffers Held Peak:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Huge Buffers Requested:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transport Frag Count:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transport Frag Peak:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transport Sends w/Flow Off:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Send Errs:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Send Peer Errs:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rcv Xform Errs:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Xmit Xform Errs:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incompatible Messages:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client Unbundles to Process Memory:</td>
<td>T</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

--------------------------------------------------------------------------------

<table>
<thead>
<tr>
<th>Client Name</th>
<th>Client</th>
<th>Entity</th>
<th>Bundle</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ID</td>
<td>ID</td>
<td>Mode</td>
</tr>
</tbody>
</table>
--------------------------------------------------------------------------------

<table>
<thead>
<tr>
<th>Online Diags HA</th>
<th>14</th>
<th>--</th>
<th>Off</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total API Messages Sent:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total Transport Messages Sent:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Length of Sent Messages:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total Blocked Messages Sent:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Length of Sent Blocked Messages:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total Non-blocked Messages Sent:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Length of Sent Non-blocked Messages:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total Bytes Allocated:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Buffers Held:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Buffers Held Peak:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Huge Buffers Requested:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transport Frag Count:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transport Frag Peak:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transport Sends w/Flow Off:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Send Errs:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Send Peer Errs:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rcv Xform Errs:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Xmit Xform Errs:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incompatible Messages:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client Unbundles to Process Memory:</td>
<td>T</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
--------------------------------------------------------------------------------

<table>
<thead>
<tr>
<th>Client Name</th>
<th>Client</th>
<th>Entity</th>
<th>Bundle</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ID</td>
<td>ID</td>
<td>Mode</td>
</tr>
</tbody>
</table>
--------------------------------------------------------------------------------

<table>
<thead>
<tr>
<th>ARP</th>
<th>22</th>
<th>--</th>
<th>Off</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total API Messages Sent:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total Transport Messages Sent:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Length of Sent Messages:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total Blocked Messages Sent:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Length of Sent Blocked Messages:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total Non-blocked Messages Sent:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Length of Sent Non-blocked Messages:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total Bytes Allocated:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Buffers Held:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Buffers Held Peak:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client Name</td>
<td>Client Entity</td>
<td>Bundle</td>
<td></td>
</tr>
<tr>
<td>-------------</td>
<td>---------------</td>
<td>--------</td>
<td></td>
</tr>
<tr>
<td>TableId CF</td>
<td>27</td>
<td>Off</td>
<td></td>
</tr>
<tr>
<td>Client Name</td>
<td>Client Entity</td>
<td>Bundle</td>
<td></td>
</tr>
<tr>
<td>Event Manager</td>
<td>33</td>
<td>Off</td>
<td></td>
</tr>
</tbody>
</table>

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
### LAN-Switch Port Man 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

### 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

### 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.

<table>
<thead>
<tr>
<th>Entity ID</th>
<th>Entity Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>CHKPT_DEFAULT_ENTITY</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Client ID</th>
<th>Client Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>168</td>
<td>DHCP Snooping</td>
</tr>
<tr>
<td>167</td>
<td>IGMP Snooping</td>
</tr>
<tr>
<td>41</td>
<td>Spanning-tree</td>
</tr>
<tr>
<td>40</td>
<td>AUTH MGR CHKPT CLIEN</td>
</tr>
<tr>
<td>39</td>
<td>LAN-Switch VLANs</td>
</tr>
<tr>
<td>33</td>
<td>Event Manager</td>
</tr>
<tr>
<td>35</td>
<td>LAN-Switch Port Mana</td>
</tr>
<tr>
<td>36</td>
<td>LAN-Switch PAgP/LACP</td>
</tr>
<tr>
<td>158</td>
<td>Inline Power Checkpoint</td>
</tr>
</tbody>
</table>

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
Buffers Held Peak: 0
show checkpoint

Current Buffers Held: 0
Huge Buffers Requested: 0
**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.

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>Privileged Mode.</td>
</tr>
<tr>
<td>Command History</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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 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
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>export-ids netflow-v9</strong></td>
<td>(Optional) Displays the NetFlow Version 9 export fields that can be exported and their IDs.</td>
</tr>
<tr>
<td><strong>name</strong></td>
<td>(Optional) Specifies the name of a flow exporter.</td>
</tr>
<tr>
<td><strong>exporter-name</strong></td>
<td>(Optional) Name of a flow exporter that was previously configured.</td>
</tr>
<tr>
<td><strong>statistics</strong></td>
<td>(Optional) Displays statistics for all flow exporters or for the specified flow exporter.</td>
</tr>
<tr>
<td><strong>templates</strong></td>
<td>(Optional) Displays template information for all flow exporters or for the specified flow exporter.</td>
</tr>
</tbody>
</table>

**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 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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 10: show flow exporter Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flow Exporter</td>
<td>The name of the flow exporter that you configured.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Description</td>
<td>The description that you configured for the exporter, or the default description User defined.</td>
</tr>
<tr>
<td>Transport Configuration</td>
<td>The transport configuration fields for this exporter.</td>
</tr>
<tr>
<td>Destination IP address</td>
<td>The IP address of the destination host.</td>
</tr>
<tr>
<td>Source IP address</td>
<td>The source IP address used by the exported packets.</td>
</tr>
<tr>
<td>Transport Protocol</td>
<td>The transport layer protocol used by the exported packets.</td>
</tr>
<tr>
<td>Destination Port</td>
<td>The destination UDP port to which the exported packets are sent.</td>
</tr>
<tr>
<td>Source Port</td>
<td>The source UDP port from which the exported packets are sent.</td>
</tr>
<tr>
<td>DSCP</td>
<td>The differentiated services code point (DSCP) value.</td>
</tr>
<tr>
<td>TTL</td>
<td>The time-to-live value.</td>
</tr>
<tr>
<td>Output Features</td>
<td>Specifies whether the output-features command, which causes the output features to be run on Flexible NetFlow export packets, has been used or not.</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 11: show flow interface Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The interface to which the information applies.</td>
</tr>
<tr>
<td>monitor</td>
<td>The name of the flow monitor that is configured on the interface.</td>
</tr>
<tr>
<td>direction</td>
<td>The direction of traffic that is being monitored by the flow monitor. The possible values are:</td>
</tr>
<tr>
<td></td>
<td>• Input—Traffic is being received by the interface.</td>
</tr>
<tr>
<td></td>
<td>• Output—Traffic is being transmitted by the interface.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>traffic(ip)</td>
<td>Indicates if the flow monitor is in normal mode or sampler mode.</td>
</tr>
<tr>
<td></td>
<td>The possible values are:</td>
</tr>
<tr>
<td></td>
<td>• on—The flow monitor is in normal mode.</td>
</tr>
<tr>
<td></td>
<td>• sampler—The flow monitor is in sampler mode (the name of the sampler will be included in the display).</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>name</strong></td>
<td>(Optional) Specifies the name of a flow monitor.</td>
</tr>
<tr>
<td><strong>monitor-name</strong></td>
<td>(Optional) Name of a flow monitor that was previously configured.</td>
</tr>
<tr>
<td><strong>cache</strong></td>
<td>(Optional) Displays the contents of the cache for the flow monitor.</td>
</tr>
<tr>
<td><strong>format</strong></td>
<td>(Optional) Specifies the use of one of the format options for formatting the display output.</td>
</tr>
<tr>
<td><strong>aggregate</strong></td>
<td>(Optional) Displays an aggregate of the given fields.</td>
</tr>
<tr>
<td><strong>filter</strong></td>
<td>(Optional) Filters and displays only matching flow records.</td>
</tr>
<tr>
<td><strong>sort</strong></td>
<td>(Optional) Sorts the resulting flow records in the required order.</td>
</tr>
<tr>
<td><strong>csv</strong></td>
<td>(Optional) Displays the flow monitor cache contents in comma-separated variables (CSV) format.</td>
</tr>
<tr>
<td><strong>record</strong></td>
<td>(Optional) Displays the flow monitor cache contents in record format.</td>
</tr>
<tr>
<td><strong>table</strong></td>
<td>(Optional) Displays the flow monitor cache contents in table format.</td>
</tr>
<tr>
<td><strong>statistics</strong></td>
<td>(Optional) Displays the statistics for the flow monitor.</td>
</tr>
</tbody>
</table>

### Command Modes

Privileged EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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 use 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
```
This table describes the significant fields shown in the display.

### Table 12: `show flow monitor monitor-name` Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flow Monitor</td>
<td>Name of the flow monitor that you configured.</td>
</tr>
<tr>
<td>Description</td>
<td>Description that you configured or the monitor, or the default description User defined.</td>
</tr>
<tr>
<td>Flow Record</td>
<td>Flow record assigned to the flow monitor.</td>
</tr>
<tr>
<td>Flow Exporter</td>
<td>Exporters that are assigned to the flow monitor.</td>
</tr>
<tr>
<td>Cache</td>
<td>Information about the cache for the flow monitor.</td>
</tr>
<tr>
<td>Type</td>
<td>Flow monitor cache type. The value is always normal, as it is the only supported cache type.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the flow monitor cache. The possible values are:</td>
</tr>
<tr>
<td></td>
<td>• allocated—The cache is allocated.</td>
</tr>
<tr>
<td></td>
<td>• being deleted—The cache is being deleted.</td>
</tr>
<tr>
<td></td>
<td>• not allocated—The cache is not allocated.</td>
</tr>
<tr>
<td>Size</td>
<td>Current cache size.</td>
</tr>
<tr>
<td>Inactive Timeout</td>
<td>Current value for the inactive timeout in seconds.</td>
</tr>
<tr>
<td>Active Timeout</td>
<td>Current value for the active timeout in seconds.</td>
</tr>
</tbody>
</table>

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.
- **record-name** (Optional) Name of a user-defined flow record that was previously configured.

**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 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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 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|inactive]|trunk]
```

**Syntax Description**

- **interface-id**  
  (Optional) ID of the interface. Valid interfaces include physical ports (including type, stack member for stacking-capable switches, module, and port number) and port channels. The port channel range is 1 to 48.

- **vlan vlan-id**  
  (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 number**  
  (Optional) Displays capabilities of all interfaces on the switch or specified stack member.  
  The range is 1 to 9.  
  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.

**inactive**  
(Optional) Displays interfaces in an inactive 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 switch in the stack. If there is no switch 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

Device# show interfaces gigabitethernet1/0/2 capabilities
GigabitEthernet1/0/2
  Model:           UA-3850-24-CR
  Type:            10/100/1000BaseTX
  Speed:           10,100,1000,auto
  Duplex:          full,half,auto
  Trunk encap. type: 802.1Q
  Trunk mode:      on,off,desirable,negotiate
  Channel:         yes
  Fast Start:      yes
  QoS scheduling:  rx-(not configurable on per port basis),
                 tx-(4q3t) (3t: Two configurable values and one fixed.)
  CoS rewrite:     yes
  ToS rewrite:     yes
  UDLD:            yes
  Inline power:    no
  SPAN:            source/destination
  PortSecure:      yes
  Dot1x:           yes

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 ip

To view the IP information, use the **show ip** command.

```yaml
show ip {access-lists | interface brief | route | tunnel [eogre {domain | forwarding-table | gateway} | fabric | summary]}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-lists</td>
<td>Lists the IP access lists</td>
</tr>
<tr>
<td>interface</td>
<td>Displays the IP interface status and configuration</td>
</tr>
<tr>
<td>brief</td>
<td>Displays the brief summary of IP status and configuration</td>
</tr>
<tr>
<td>route</td>
<td>Displays the IP routing table</td>
</tr>
<tr>
<td>tunnel</td>
<td>Displays the IP tunnel information</td>
</tr>
<tr>
<td>eogre</td>
<td>Displays the EoGRE tunnel information</td>
</tr>
<tr>
<td>domain</td>
<td>Displays the EoGRE tunnel domain information</td>
</tr>
<tr>
<td>forwarding-table</td>
<td>Displays the EoGRE tunnel encapsulation and decapsulation information</td>
</tr>
<tr>
<td>gateway</td>
<td>Displays the EoGRE tunnel gateway information</td>
</tr>
<tr>
<td>fabric</td>
<td>Displays the IP fabric tunnel information</td>
</tr>
<tr>
<td>summary</td>
<td>Displays the information for all tunnels</td>
</tr>
</tbody>
</table>

**Command Modes**

- User EXEC (>)
- Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.111.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

The following example shows how to view information about the lists the IP access lists:

```
cisco-wave2-ap# show ip access-lists
```
show ip device tracking

To display information about entries in the IP device tracking table, use the show ip device tracking command in privileged EXEC mode.

```
show ip device tracking {all count|interface type-of-interface|ip ip-address|mac mac-address}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all count</td>
<td>Displays a count of all IP tracking host entries.</td>
</tr>
<tr>
<td>interface</td>
<td>Displays interface information. See the table below for a list of valid interfaces.</td>
</tr>
<tr>
<td>ip ip-address</td>
<td>Displays the IP address of the client.</td>
</tr>
<tr>
<td>mac mac-address</td>
<td>Displays the 48-bit hardware MAC address.</td>
</tr>
</tbody>
</table>

### Command Modes

Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2SX</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.4(15)T</td>
<td>This command was integrated into Cisco IOS Release 12.4(15)T.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The table below displays valid interfaces that may be shown as the type-of-interface argument with the interface keyword.

#### Table 13: Interfaces That Can Be Tracked

<table>
<thead>
<tr>
<th>Interface</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Async</td>
<td>Asynchronous interface</td>
</tr>
<tr>
<td>BVI</td>
<td>Bridge-Group Virtual Interface</td>
</tr>
<tr>
<td>CDMA-Ix</td>
<td>CDMA Ix interface</td>
</tr>
<tr>
<td>CTunnel</td>
<td>CTunnel interface</td>
</tr>
<tr>
<td>Dialer</td>
<td>Dialer interface</td>
</tr>
<tr>
<td>FastEthernet</td>
<td>FastEthernet IEEE 802.3</td>
</tr>
<tr>
<td>Lex</td>
<td>Lex interface</td>
</tr>
<tr>
<td>Loopback</td>
<td>Loopback interface</td>
</tr>
<tr>
<td>MFR</td>
<td>Multilink Frame Relay bundle intrface</td>
</tr>
<tr>
<td>Multilink</td>
<td>Multilink-group interface</td>
</tr>
</tbody>
</table>
### Interface Table

<table>
<thead>
<tr>
<th>Interface</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Null</td>
<td>Null interface</td>
</tr>
<tr>
<td>Port-channel</td>
<td>Ethernet channel of interfaces</td>
</tr>
<tr>
<td>Serial</td>
<td>Serial</td>
</tr>
<tr>
<td>Tunnel</td>
<td>Tunnel interface</td>
</tr>
<tr>
<td>vif</td>
<td>Pragmatic General Multicast (PGM) multicast host interface</td>
</tr>
<tr>
<td>virtual</td>
<td>Virtual interface</td>
</tr>
<tr>
<td>virtual-PPP</td>
<td>Virtual PPP interface</td>
</tr>
<tr>
<td>virtual-Template</td>
<td>Virtual template interface</td>
</tr>
<tr>
<td>virtual-TokenRing</td>
<td>Virtual TokenRing</td>
</tr>
<tr>
<td>XTagATM</td>
<td>Extended Tag ATM interface</td>
</tr>
</tbody>
</table>

### Examples

The following example shows that all host entries are to be tracked:

```bash
Router# show ip device tracking all count
IP Device Tracking = Enabled
Probe Count: 2
Probe Interval: 10
```

The fields in the above display are self-explanatory.
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.

**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 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan  vlan-id</td>
<td>(Optional) Specifies a VLAN; Ranges are from 1—1001 and 1006—4094.</td>
</tr>
<tr>
<td>detail</td>
<td>(Optional) Displays detailed IGMP querier information.</td>
</tr>
</tbody>
</table>

**Command Modes**

User EXEC
Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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:

```plaintext
Device> show ip igmp snooping querier detail

<table>
<thead>
<tr>
<th>Vlan</th>
<th>IP Address</th>
<th>IGMP Version</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1.1.1.1</td>
<td>v2</td>
<td>Fa8/0/1</td>
</tr>
</tbody>
</table>

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 1.1.1.1 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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>wlan-name</td>
<td>Name of the WLAN.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Command Modes</th>
<th>Privileged EXEC</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
</tr>
</tbody>
</table>

**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**

- `access-list-name` (Optional) Name of access list.

**Command Default**

All IPv6 access lists are displayed.

**Command Modes**

User EXEC

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>

**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 14: `show ipv6 access-list` Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 access list inbound</td>
<td>Name of the IPv6 access list, for example, inbound.</td>
</tr>
<tr>
<td>permit</td>
<td>Permits any packet that matches the specified protocol type.</td>
</tr>
<tr>
<td>tcp</td>
<td>Transmission Control Protocol. The higher-level (Layer 4) protocol type that the packet must match.</td>
</tr>
<tr>
<td>any</td>
<td>Equal to ::/0.</td>
</tr>
<tr>
<td>eq</td>
<td>An equal operand that compares the source or destination ports of TCP or UDP packets.</td>
</tr>
<tr>
<td>bgp</td>
<td>Border Gateway Protocol. The lower-level (Layer 3) protocol type that the packet must be equal to.</td>
</tr>
<tr>
<td>reflect</td>
<td>Indicates a reflexive IPv6 access list.</td>
</tr>
<tr>
<td>tcptraffic (8 matches)</td>
<td>The name of the reflexive IPv6 access list and the number of matches for the access list. The <strong>clear ipv6 access-list</strong> privileged EXEC command resets the IPv6 access list match counters.</td>
</tr>
<tr>
<td>sequence 10</td>
<td>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).</td>
</tr>
<tr>
<td>host 2001:0DB8:1::1</td>
<td>The source IPv6 host address that the source address of the packet must match.</td>
</tr>
<tr>
<td>host 2001:0DB8:1::2</td>
<td>The destination IPv6 host address that the destination address of the packet must match.</td>
</tr>
<tr>
<td>11000</td>
<td>The ephemeral source port number for the outgoing connection.</td>
</tr>
<tr>
<td>timeout 300</td>
<td>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.</td>
</tr>
<tr>
<td>(time left 243)</td>
<td>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.</td>
</tr>
<tr>
<td>evaluate udptraffic</td>
<td>Indicates the IPv6 reflexive access list named udptraffic is nested in the IPv6 access list named outbound.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ipv6 access-list</td>
<td>Resets the IPv6 access list match counters.</td>
</tr>
<tr>
<td>hardware statistics</td>
<td>Enables the collection of hardware statistics.</td>
</tr>
<tr>
<td>show ip access-list</td>
<td>Displays the contents of all current IP access lists.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>show ip prefix-list</code></td>
<td>Displays information about a prefix list or prefix list entries.</td>
</tr>
<tr>
<td><code>show ipv6 prefix-list</code></td>
<td>Displays information about an IPv6 prefix list or IPv6 prefix list entries.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vlan</code></td>
<td>(Optional) Specify a VLAN; the range is 1 to 1001 and 1006 to 4094.</td>
</tr>
</tbody>
</table>

**Command Modes**

- User EXEC
- 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>

**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

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
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 mld snooping</td>
<td>Enables and configures MLD snooping on the switch or on a VLAN.</td>
</tr>
<tr>
<td>sdm prefer</td>
<td>Configures an SDM template to optimize system resources based on how the switch is being used.</td>
</tr>
</tbody>
</table>
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**

*vlan-id*  
VLAN ID. Valid range is 1 to 1001 and 1006 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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**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
```

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>Privileged EXEC</td>
</tr>
<tr>
<td>Command History</td>
<td><strong>Release</strong></td>
</tr>
<tr>
<td></td>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
</tr>
</tbody>
</table>

**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
```

---

Cisco Catalyst 9800 Series Wireless Controller Command Reference, Cisco IOS XE Gibraltar 16.10.x
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** 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-con
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          String DN element-req-qos
department             String DN element-req-qos
```
show ldap server

To view the LDAP server state information and various other counters for the server, use the `show ldap server` command.

```
show ldap server
```

**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>

This example shows how to view the LDAP server state information and various other counters for the server:

```
Device# show ldap server
```
**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]}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Option to enter the EID table.</th>
</tr>
</thead>
<tbody>
<tr>
<td>eid-table</td>
<td></td>
</tr>
<tr>
<td>default</td>
<td>Shows the information for the default VRF.</td>
</tr>
<tr>
<td>vlan vlan-id</td>
<td>Enter the VLAN information.</td>
</tr>
<tr>
<td>vrf vrf-name</td>
<td>Enter the VRF name.</td>
</tr>
<tr>
<td>instance-id id-number</td>
<td>Enter the EID instance ID.</td>
</tr>
<tr>
<td>internal</td>
<td>Shows the site's detailed internal information.</td>
</tr>
</tbody>
</table>

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**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.

**Syntax Description**

```
show logging profile wireless end timestamp  time-stamp
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>time-stamp</strong></td>
<td>Time to end the filtering. For example, 2017/02/10 14:41:50.849.</td>
</tr>
</tbody>
</table>

**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>

**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**

<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>

**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**

<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>

**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**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>This command has no keywords or arguments.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Default</td>
<td>None</td>
</tr>
<tr>
<td>Command Modes</td>
<td>Privileged EXEC (#)</td>
</tr>
<tr>
<td>Command History</td>
<td></td>
</tr>
<tr>
<td>Release</td>
<td>Modification</td>
</tr>
<tr>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<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>

**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
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>module-name</th>
<th>A comma or space separated list of module names. For example, dbal, tdllib or &quot;dbal tdllib&quot;.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Default</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Command Modes</td>
<td>Privileged EXEC (#)</td>
<td></td>
</tr>
<tr>
<td>Command History</td>
<td>Release</td>
<td>Modification</td>
</tr>
<tr>
<td></td>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 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**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>This command has no keywords or arguments.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Default</td>
<td>None</td>
</tr>
<tr>
<td>Command Modes</td>
<td>Privileged EXEC (#)</td>
</tr>
<tr>
<td>Command History</td>
<td><strong>Release</strong></td>
</tr>
<tr>
<td></td>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
</tr>
</tbody>
</table>

**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 }
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>marker</td>
<td>The marker to start filtering from. It must match with previously set marker.</td>
</tr>
<tr>
<td>timestamp</td>
<td>The timestamp for filtering. For example, &quot;2017/02/10 14:41:50.849&quot;.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>Privileged EXEC (#)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Usage Guidelines</th>
<th>Ensure that you enable <code>internal</code> keyword using the <code>show logging profile wireless internal</code> command to get the trace output.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Without the <code>internal</code> keyword, only customer curated logs are displayed.</td>
</tr>
</tbody>
</table>

**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}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>switch-num</code></td>
</tr>
<tr>
<td><code>active</code></td>
</tr>
<tr>
<td><code>standby</code></td>
</tr>
</tbody>
</table>

**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>

**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 switch 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**

<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>

**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 mac access-group

To display the MAC access control lists (ACLs) configured for an interface or a switch, use the `show mac access-group` command in EXEC mode.

`show mac access-group [interface interface-id]`

**Syntax Description**

| interface interface-id | (Optional) Display the MAC ACLs configured on a specific interface. Valid interfaces are physical ports and port channels; the port-channel range is 1 to 48 (available only in privileged EXEC mode). |

**Command Modes**

- User EXEC
- Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

This is a sample output from the `show mac access-group` command in EXEC mode. In this display, port 2 has the MAC access list `macl_e1` applied; no MAC ACLs are applied to other interfaces.

```
Device# show mac access-group

Interface GigabitEthernet1/0/1:
  Inbound access-list is not set
Interface GigabitEthernet1/0/2:
  Inbound access-list is macl_e1
Interface GigabitEthernet1/0/3:
  Inbound access-list is not set
Interface GigabitEthernet1/0/4:
  Inbound access-list is not set
<output truncated>
```

This is a sample output from the `show mac access-group interface gigabitethernet1/0/1` command:

```
Device# show mac access-group interface gigabitethernet1/0/1

Interface GigabitEthernet1/0/1:
  Inbound access-list is macl_e1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac access-group</td>
<td>Applies a MAC access group to an interface.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ap</code></td>
<td>Displays information about the access point.</td>
</tr>
<tr>
<td><code>ip-address</code></td>
<td>(Optional) IP address.</td>
</tr>
<tr>
<td><code>mn</code></td>
<td>Displays information about the mobile node.</td>
</tr>
<tr>
<td><code>ip</code></td>
<td>(Optional) Displays information about the IP database thread.</td>
</tr>
<tr>
<td><code>ip-address</code></td>
<td></td>
</tr>
<tr>
<td><code>mac</code></td>
<td>Displays information about the MAC database thread.</td>
</tr>
<tr>
<td><code>mac-address</code></td>
<td></td>
</tr>
<tr>
<td><code>network</code></td>
<td>Displays information for a specific wireless network ID.</td>
</tr>
<tr>
<td><code>network-id</code></td>
<td></td>
</tr>
<tr>
<td><code>status</code></td>
<td>Displays status information.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(18)SXD</td>
<td>This command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(18)SXD3</td>
<td>The output of this command was changed to include the TCP adjust-mss status.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**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.8fa.85c9 10.1.3.11 172.16.1.2 103
```
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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>mobility</code></td>
<td>Configures the wireless mGRE tunnels.</td>
</tr>
</tbody>
</table>
show nmsp

To display the Network Mobility Services Protocol (NMSP) configuration settings, use the `show nmsp` command.

```
show nmsp {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 3.2SE  This command was introduced.

The following is sample output from the `show nmsp notification interval` command:

```
Device# show nmsp 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**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to see NMSP cloud-service statistics:

```
Device# show nmsp cloud-services statistics
```
show nmsp cloud-services summary

To see a summary of information about NMSP cloud-services, use the `show nmsp cloud-services summary` command.

```
show nmsp cloud-services summary [chassis {chassis-number | active | standby} R0]
```

**Syntax Description**

- **chassis-number** 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>
<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>

**Examples**

This example shows how to see NMSP cloud-service summary information:

```
Device# show nmsp cloud-services summary
```
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group-name</td>
<td>CMX AP group name.</td>
</tr>
<tr>
<td>cmx-IP-address</td>
<td>CMX IP address.</td>
</tr>
</tbody>
</table>

**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>

**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 00:00:00:00:00:02 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 00:00:00:00:00:02 00:00:00:00:00:02 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**

- `group-name` CMX AP group name.
- `cmx-IP-address` CMX IP address.

**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>

**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.

**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>

**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 platform conditions

To see information about conditional debugs, use the `show platform conditions` command.

```
show platform conditions
```

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>Privileged EXEC</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release</td>
</tr>
<tr>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
</tr>
</tbody>
</table>

**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}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>active</td>
<td>Active instance.</td>
</tr>
<tr>
<td>qfp</td>
<td>Quantum Flow Processor.</td>
</tr>
<tr>
<td>wlclient</td>
<td>QFP wireless client.</td>
</tr>
<tr>
<td>cpp-if-handle</td>
<td>client cpp interface handle.</td>
</tr>
<tr>
<td>client-cpp-value</td>
<td>Client cpp if-handle value. The range is between 1 and 4294967295.</td>
</tr>
<tr>
<td>statistics</td>
<td>Show Client Statistics.</td>
</tr>
<tr>
<td>clear</td>
<td>Shows and Clears the Client Statistics.</td>
</tr>
<tr>
<td>start</td>
<td>Start Client Statistics collection.</td>
</tr>
<tr>
<td>stop</td>
<td>Stop Client Statistics collection.</td>
</tr>
</tbody>
</table>

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**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.

**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 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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.
- `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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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: urllist_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.

**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 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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: urlist_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
```

Syntax Description

- **address** `[ipv4 ipv4_address | ipv6 ipv6_address]` | **all** | **pattern regex_pattern**
  - Displays the DSA address entry details
  - Displays all the DSA IP cache address details
  - Displays the DSA IP cache pattern details

Command Default

None

Command Modes

Global configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
</table>
| Cisco IOS XE 3.2SE | 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*
IP Addresses matching pattern .*google*
IP Address Client(s) Expire Match RegexId Dirty
2607:f8b0:14004:8000:0:0:0:2004 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.

### 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 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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.

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent datapath regexp-table
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>This command has no arguments.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Default</td>
<td>None</td>
</tr>
<tr>
<td>Command Modes</td>
<td>Global configuration</td>
</tr>
<tr>
<td>Command History</td>
<td></td>
</tr>
<tr>
<td>Release</td>
<td>Modification</td>
</tr>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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 MLS_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.

```
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.

```
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.

```
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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 SPLIT 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.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>This command has no arguments.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Default</td>
<td>None</td>
</tr>
<tr>
<td>Command Modes</td>
<td>Global configuration</td>
</tr>
<tr>
<td>Command History</td>
<td></td>
</tr>
<tr>
<td>Release</td>
<td>Modification</td>
</tr>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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.

```
Device# show platform hardware chassis active qfp feature wireless et-analytics eta-pending-client-tree
CPP IF_H DPIX 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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 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 mac-address` 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Denali 16.1.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command collates and sorts all the logs present in the `/tmp/.../` 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 `collated_log_{system time}` with the same content, in the `/crashinfo/tracelogs` 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**

<table>
<thead>
<tr>
<th>Context</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>context mac-address</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Command Modes**

- User EXEC (>)
- Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Denali 16.1.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command collates and sorts all the logs present in the /tmp/.../ 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 collated_log_{system time} with the same content, in the /crashinfo/tracelogs 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  process  slot`

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>process</th>
<th>Process whose tracing level is being set. Options include:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>chassis-manager</td>
<td>The Chassis Manager process.</td>
</tr>
<tr>
<td></td>
<td>cli-agent</td>
<td>The CLI Agent process.</td>
</tr>
<tr>
<td></td>
<td>cmm</td>
<td>The CMM process.</td>
</tr>
<tr>
<td></td>
<td>dbm</td>
<td>The Database Manager process.</td>
</tr>
<tr>
<td></td>
<td>emd</td>
<td>The Environmental Monitoring process.</td>
</tr>
<tr>
<td></td>
<td>fed</td>
<td>The Forwarding Engine Driver process.</td>
</tr>
<tr>
<td></td>
<td>forwarding-manager</td>
<td>The Forwarding Manager process.</td>
</tr>
<tr>
<td></td>
<td>geo</td>
<td>The Geo Manager process.</td>
</tr>
<tr>
<td></td>
<td>host-manager</td>
<td>The Host Manager process.</td>
</tr>
<tr>
<td></td>
<td>interface-manager</td>
<td>The Interface Manager process.</td>
</tr>
<tr>
<td></td>
<td>iomd</td>
<td>The Input/Output Module daemon (IOMd) process.</td>
</tr>
<tr>
<td></td>
<td>ios</td>
<td>The IOS process.</td>
</tr>
<tr>
<td></td>
<td>license-manager</td>
<td>The License Manager process.</td>
</tr>
<tr>
<td></td>
<td>logger</td>
<td>The Logging Manager process.</td>
</tr>
<tr>
<td></td>
<td>platform-mgr</td>
<td>The Platform Manager process.</td>
</tr>
<tr>
<td></td>
<td>pluggable-services</td>
<td>The Pluggable Services process.</td>
</tr>
<tr>
<td></td>
<td>replication-mgr</td>
<td>The Replication Manager process.</td>
</tr>
<tr>
<td></td>
<td>shell-manager</td>
<td>The Shell Manager process.</td>
</tr>
<tr>
<td></td>
<td>sif</td>
<td>The Stack Interface (SIF) Manager process.</td>
</tr>
<tr>
<td></td>
<td>smd</td>
<td>The Session Manager process.</td>
</tr>
<tr>
<td></td>
<td>stack-mgr</td>
<td>The Stack Manager process.</td>
</tr>
<tr>
<td></td>
<td>table-manager</td>
<td>The Table Manager Server.</td>
</tr>
<tr>
<td></td>
<td>thread-test</td>
<td>The Multithread Manager process.</td>
</tr>
<tr>
<td></td>
<td>virt-manager</td>
<td>The Virtualization Manager process.</td>
</tr>
<tr>
<td></td>
<td>wireless</td>
<td>The wireless controller module process.</td>
</tr>
</tbody>
</table>
Hardware slot where the process for which the trace level is set, is running. Options include:

- **number**—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.

- **SIP-slot / SPA-bay**—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.

  - **number**—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.

  - **SIP-slot / SPA-bay**—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.

### Command Modes

- User EXEC (>)
- Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Denali 16.1.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

This example shows how to view the trace level:

```
Device# show platform software trace level dbm switch active R0
```
<table>
<thead>
<tr>
<th>Module Name</th>
<th>Trace Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>binos</td>
<td>Notice</td>
</tr>
<tr>
<td>binos/brand</td>
<td>Notice</td>
</tr>
<tr>
<td>bipc</td>
<td>Notice</td>
</tr>
<tr>
<td>btrace</td>
<td>Notice</td>
</tr>
<tr>
<td>bump_ptr_alloc</td>
<td>Notice</td>
</tr>
<tr>
<td>cdllib</td>
<td>Notice</td>
</tr>
<tr>
<td>chasfs</td>
<td>Notice</td>
</tr>
<tr>
<td>dbal</td>
<td>Informational</td>
</tr>
<tr>
<td>dbm</td>
<td>Debug</td>
</tr>
<tr>
<td>evlib</td>
<td>Notice</td>
</tr>
<tr>
<td>evutil</td>
<td>Notice</td>
</tr>
<tr>
<td>file_alloc</td>
<td>Notice</td>
</tr>
<tr>
<td>green-be</td>
<td>Notice</td>
</tr>
<tr>
<td>ios-avl</td>
<td>Notice</td>
</tr>
<tr>
<td>klib</td>
<td>Debug</td>
</tr>
<tr>
<td>services</td>
<td>Notice</td>
</tr>
<tr>
<td>sw_wdog</td>
<td>Notice</td>
</tr>
<tr>
<td>syswh</td>
<td>Notice</td>
</tr>
<tr>
<td>tdl_cdlcore_message</td>
<td>Notice</td>
</tr>
<tr>
<td>tdl_dbal_root_message</td>
<td>Notice</td>
</tr>
<tr>
<td>tdl_dbal_root_type</td>
<td>Notice</td>
</tr>
</tbody>
</table>
show platform software trace message

To display the trace messages for a process, use the set platform software trace command in privileged EXEC or user EXEC mode.

show platform software trace message process slot
<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>process</th>
</tr>
</thead>
</table>

Tracing level that 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.
<table>
<thead>
<tr>
<th>slot</th>
<th>Hardware slot where the process for which the trace level is set, is running. Options include:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• <strong>number</strong>—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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>SIP-slot / SPA-bay</strong>—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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>F0</strong>—The Embedded Service Processor slot 0.</td>
</tr>
<tr>
<td></td>
<td>• <strong>FP active</strong>—The active Embedded Service Processor.</td>
</tr>
<tr>
<td></td>
<td>• <strong>R0</strong>—The route processor in slot 0.</td>
</tr>
<tr>
<td></td>
<td>• <strong>RP active</strong>—The active route processor.</td>
</tr>
<tr>
<td></td>
<td>• <strong>switch &lt;number&gt;</strong>—The switch, with its number specified.</td>
</tr>
<tr>
<td></td>
<td>• <strong>switch active</strong>—The active switch.</td>
</tr>
<tr>
<td></td>
<td>• <strong>switch standby</strong>—The standby switch.</td>
</tr>
<tr>
<td></td>
<td>• <strong>number</strong>—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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>SIP-slot / SPA-bay</strong>—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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>F0</strong>—The Embedded Service Processor in slot 0.</td>
</tr>
<tr>
<td></td>
<td>• <strong>FP active</strong>—The active Embedded Service Processor.</td>
</tr>
<tr>
<td></td>
<td>• <strong>R0</strong>—The route processor in slot 0.</td>
</tr>
<tr>
<td></td>
<td>• <strong>RP active</strong>—The active route processor.</td>
</tr>
</tbody>
</table>

**Command Modes**

- User EXEC (>)
- Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Denali 16.1.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
This example shows how to display the trace messages for the Stack Manager and the Forwarding Engine Driver processes:

Device# show platform software trace message stack-mgr switch active R0
10/30 09:42:48.767 [btrace] [8974]: (note): Successfully registered module [97] [uiutil]
[tdd_cdlcore_message]
10/29 13:28:19.023 [stack_mgr] [8974]: (note): Examining peer state
10/29 13:28:19.022 [stack_mgr] [8974]: (note): Posting event
stack_fsm_event_wait_standby_elect_timer_expired, curstate stack_fsm_state_active_ready
10/29 13:28:19.022 [stack_mgr] [8974]: (note): Timer HDL - STACK_WAIT_STANDBY_ELECT_TIMER expired
10/29 13:28:19.022 [btrace] [8974]: (note): Successfully registered module [98] [tdl_cdlcore_message]
10/29 13:26:46.584 [btrace] [8974]: (note): Successfully registered module [99] [tdl_ui_message]
10/29 13:26:46.582 [bipc] [8974]: (note): Pending connection to server 10.129.1.0
10/29 13:26:36.582 [evutil] [8974]: (ERR): Connection attempt for sman-ui-serv (uipeer uplink to slot 1) failed, invoking disconnect
10/29 13:26:36.582 [evutil] [8974]: (ERR): Asynchronous connect failed for [uipeer uplink to slot 1] (fd == -1)
10/29 13:26:36.581 [bipc] [8974]: (note): Pending connection to server 10.129.1.0
10/29 13:26:26.581 [evutil] [8974]: (ERR): Connection attempt for sman-ui-serv (uipeer uplink to slot 1) failed, invoking disconnect

Device# show platform software trace message fed switch active
11/02 10:55:01.832 [btrace]: [11310]: UUID: 0, ra: 0 (note): Successfully registered module [86] [uiutil]
11/02 10:55:01.848 [btrace]: [11310]: UUID: 0, ra: 0 (note): Single message size is greater than 1024
11/02 10:55:01.822 [btrace]: [11310]: UUID: 0, ra: 0 (note): Successfully registered module [87] [tdl_cdlcore_message]
11/01 09:54:41.474 [btrace]: [12312]: UUID: 0, ra: 0 (note): Successfully registered module [88] [tdl_ngwc_gold_message]
11/01 09:54:11.228 [btrace]: [12312]: UUID: 0, ra: 0 (note): Successfully registered module [89] [tdl_doppler_iosd_matm_type]
11/01 09:53:37.454 [btrace]: [11310]: UUID: 0, ra: 0 (note): Successfully registered module [90] [tdl_ui_message]
11/01 09:53:37.382 [bipc]: [11310]: UUID: 0, ra: 0 (note): Pending connection to server 10.129.1.0
11/01 09:53:34.227 [xcvr]: [18846]: UUID: 0, ra: 0 (ERR): FRU hardware authentication Fail, result = 1.
11/01 09:53:33.775 [ng3k_scc]: [18846]: UUID: 0, ra: 0 (ERR): SMART COOKIE: SCC I2C receive failed: rc=10
11/01 09:53:33.775 [ng3k_scc]: [18846]: UUID: 0, ra: 0 (ERR): SMART COOKIE receive failed, try again
11/01 09:53:33.585 [ng3k_scc]: [18846]: UUID: 0, ra: 0 (ERR):
show platform software trace message license-manager RP

To display the trace message for license-manager process of active route processor, use the `show platform software trace message license-manager RP` command in privileged EXEC mode.

`show platform software trace message license-manager RP active`

This command has no arguments or keywords.

**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>

**Example**

This example shows how to display the trace messages for the Forwarding Engine Driver processes:

```
Device# show platform software trace message license-manager RP active
........
2018/06/25 07:16:53.121 {lman_R0-0}{1}: [btrace] [21231]: UUID: 0, ra: 0, TID: 0 (note):
  Decode of the file /tmp/rp/trace/lman_R0-0.21231_0.20180620075420.bin.copy completed in 35 msecs
/tmp/rp/trace/lman_R0-0.21231_0.20180620075420.bin.copy: DECODE(50:50:0:?)
2018/06/25 07:16:53.088 {lman_R0-0}{1}: [btrace] [21231]: UUID: 0, ra: 0, TID: 0 (note):
  Decode of file [/tmp/rp/trace/lman_R0-0.21231_0.20180620075420.bin.copy] returned [0]
2018/06/25 06:53:20.421 {lman_R0-0}{1}: [btrace] [21231]: UUID: 0, ra: 0, TID: 0 (note):
  Decode of the file /tmp/rp/trace/lman_R0-0.21231_0.20180620075420.bin.copy completed in 34 msecs
2018/06/25 06:53:20.389 {lman_R0-0}{1}: [btrace] [21231]: UUID: 0, ra: 0, TID: 0 (note):
  Decode of file [/tmp/rp/trace/lman_R0-0.21231_0.20180620075420.bin.copy] returned [0]
2018/06/20 07:55:10.540 {lman_R0-0}{1}: [trccfg] [21231]: UUID: 0, ra: 0, TID: 0 (note):
  Processing all-modules
2018/06/20 07:55:10.540 {lman_R0-0}{1}: [trccfg] [21231]: UUID: 0, ra: 0, TID: 0 (note):
  Empty trace conf file
2018/06/20 07:54:46.453 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (note):
  Constructing domain iosd_lmrp for RP/0/0 to RP/0/0
2018/06/20 07:54:46.453 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (note):
  Received registration msg from [IOS]
2018/06/20 07:54:46.449 {lman_R0-0}{1}: [bipc] [21231]: UUID: 0, ra: 0, TID: 0 (note):
  Received a connection from client for path /tmp/rp/lipc/license_mgr_socket
2018/06/20 07:54:45.557 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The ipc information for IOS is invalid
2018/06/20 07:54:44.556 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The ipc information for IOS is invalid
2018/06/20 07:54:43.556 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The ipc information for IOS is invalid
2018/06/20 07:54:42.555 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The ipc information for IOS is invalid
2018/06/20 07:54:41.554 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The ipc information for IOS is invalid
2018/06/20 07:54:40.553 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The ipc information for IOS is invalid
2018/06/20 07:54:39.553 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The ipc information for IOS is invalid
```
2018/06/20 07:54:38.552 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The ipc information for IOS is invalid
2018/06/20 07:54:37.551 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The ipc information for IOS is invalid
2018/06/20 07:54:36.550 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The ipc information for IOS is invalid
2018/06/20 07:54:35.550 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The ipc information for IOS is invalid
2018/06/20 07:54:34.549 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The ipc information for IOS is invalid
2018/06/20 07:54:33.548 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The ipc information for IOS is invalid
2018/06/20 07:54:32.547 {lman_R0-0}{1}: [bipc] [21231]: UUID: 0, ra: 0, TID: 0 (note): Pending connection to server 10.0.1.0
2018/06/20 07:54:31.547 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The ipc information for IOS is invalid
2018/06/20 07:54:30.546 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The ipc information for IOS is invalid
2018/06/20 07:54:29.545 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The ipc information for IOS is invalid
2018/06/20 07:54:28.545 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The ipc information for IOS is invalid
2018/06/20 07:54:27.545 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The ipc information for IOS is invalid
2018/06/20 07:54:26.544 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The ipc information for IOS is invalid
2018/06/20 07:54:25.543 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The ipc information for IOS is invalid
2018/06/20 07:54:24.542 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The ipc information for IOS is invalid
2018/06/20 07:54:23.542 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The ipc information for IOS is invalid
2018/06/20 07:54:22.541 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The ipc information for IOS is invalid
2018/06/20 07:54:21.540 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The ipc information for IOS is invalid
2018/06/20 07:54:20.633 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (note): Peer attach: from location R0:0 is successful
2018/06/20 07:54:20.633 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (note): Not setting domain for cmand
2018/06/20 07:54:20.625 {lman_R0-0}{1}: [bipc] [21231]: UUID: 0, ra: 0, TID: 0 (note): Received a connection from client for path /tmp/rp/lipc/lman_lic_serv_socket
2018/06/20 07:54:20.624 {lman_R0-0}{1}: [tdllib] [21231]: UUID: 0, ra: 0, TID: 0 (note): epoch file read /tmp/tdlresolve/epoch_dir//2018_06_20_07_54_2413.epoch
2018/06/20 07:54:20.624 {lman_R0-0}{1}: [tdllib] [21231]: UUID: 0, ra: 0, TID: 0 (note): Detect newly epoch file generated: new epoch: /tmp/tdlresolve/epoch_dir//2018_06_20_07_54_2413.epoch
2018/06/20 07:54:20.624 {lman_R0-0}{1}: [tdllib] [21231]: UUID: 0, ra: 0, TID: 0 (note): Detect newly epoch file generated: new epoch: /tmp/tdlresolve/epoch_dir//2018_06_20_07_54_2413.epoch
2018/06/20 07:54:20.624 {lman_R0-0}{1}: [tdllib] [21231]: UUID: 0, ra: 0, TID: 0 (note): Flag tdih stale epoch for all tdh handles
2018/06/20 07:54:20.624 {lman_R0-0}{1}: [tdllib] [21231]: UUID: 0, ra: 0, TID: 0 (note): Chassis Watch on rp/0/0/rtu_licensing for platform to create RTU properties
2018/06/20 07:54:20.536 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (note): The chassis product id: "ISR4461/K9"
2018/06/20 07:54:20.536 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (note): The chassis serial number: "FDO2213A0GL"
2018/06/20 07:54:20.536 {lman_R0-0}{1}: [bcrdu] [21231]: UUID: 0, ra: 0, TID: 0 (note): CRDU
http://sw/mount/isr4400v2-mono-universalk9.BLD_V169_THROTTLE_LATEST_20180618_044856_V16_9_0_163.SSA.pkg/usr/binos/bin/lman
proc path is /tmp/patch/CRDU/BPROC_LM_RP/
procstr is BPROC_LM_RP
2018/06/20 07:54:20.533 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (note): No licensing objects present in chasfs to delete
2018/06/20 07:54:20.533 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (note): Deleting any existing licensing chasfs objects under [rp/0/0/licensing]
2018/06/20 07:54:20.532 {lman_R0-0}{1}: [syshw] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): syshw build device: could not add register 7 dev: /sys/bus/platform/devices/cpld/reg_rp_sku_register (No such file or directory) due to No such file or directory
2018/06/20 07:54:20.532 {lman_R0-0}{1}: [syshw] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): syshw build device: could not add register 5 dev: /sys/bus/platform/devices/cpld/phys_slot_number (No such file or directory) due to No such file or directory

Total messages : 49
show platform software trace message license-manager

To display the trace message for license-manager process of router processor, use the `show platform software trace message license-manager` command in privileged EXEC mode.

**Syntax Description**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>RO</code></td>
<td>The route processor in slot 0.</td>
</tr>
</tbody>
</table>

**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>

**Example**

This example shows how to display the trace messages for the Forwarding Engine Driver processes:

```
Device# show platform software trace message license-manager R0

.......
2018/06/25 06:53:20.421 {lman_R0-0}{1}: [btrace] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Decode of the file /tmp/rp/trace/lman_R0-0.21231_0.20180620075420.bin.copy completed in 34
msecs
/tmp/rp/trace/lman_R0-0.21231_0.20180620075420.bin.copy: DECODE(48:48:0:7)
2018/06/25 06:53:20.389 {lman_R0-0}{1}: [btrace] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Decode of file [/tmp/rp/trace/lman_R0-0.21231_0.20180620075420.bin.copy] returned [0]
2018/06/20 07:55:10.540 {lman_R0-0}{1}: [trccfg] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Processing all-modules
2018/06/20 07:55:10.540 {lman_R0-0}{1}: [trccfg] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Empty trace conf file
2018/06/20 07:54:46.453 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Constructing domain iosd_imrp for RP/0/0 to RP/0/0
2018/06/20 07:54:46.453 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Received registration msg from [IOS]
2018/06/20 07:54:46.449 {lman_R0-0}{1}: [bipc] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Received a connection from client for path /tmp/rp/lipc/license_mgr_socket
2018/06/20 07:54:45.557 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:44.556 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:43.556 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:42.555 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:41.554 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:40.553 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:39.553 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:38.552 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
```
licensing objects present in chasfs to delete
2018/06/20 07:54:20.533 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Deleting any existing licensing chasfs objects under [rp/0/0/licensing]
2018/06/20 07:54:20.532 {lman_R0-0}{1}: [syshw] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): syshw
build device: could not add register 7 dev: /sys/bus/platform/devices/cpld/reg_rp_sku_register (No such file or directory) due to No such file or directory
2018/06/20 07:54:20.532 {lman_R0-0}{1}: [syshw] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): syshw
build device: could not add register 5 dev: /sys/bus/platform/devices/cpld/phys_slot_number (No such file or directory) due to No such file or directory
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.

**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 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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.

**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 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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 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>

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  57CC80106C087FB1B2A7B0B4F2F4373C00247166
  local-domain dns_wl
dns_crypt
dns_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}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>policy-map-name</code></td>
<td>(Optional) Name of the policy-map.</td>
</tr>
<tr>
<td><code>interface interface-id</code></td>
<td>(Optional) Displays the statistics and the configurations of the input and output policies that are attached to the interface.</td>
</tr>
<tr>
<td><code>ap name ap_name</code></td>
<td>Displays SSID policy configuration of an access point.</td>
</tr>
<tr>
<td><code>client mac mac_address</code></td>
<td>Displays information about the policies for all the client targets.</td>
</tr>
<tr>
<td>`radio type {24ghz</td>
<td>5ghz}`</td>
</tr>
<tr>
<td><code>ssid name ssid_name</code></td>
<td>Displays policy configuration of an SSID.</td>
</tr>
</tbody>
</table>

**Command Modes**

- User EXEC
- Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE 3.3SE</td>
<td>The <code>interface interface-id</code> keyword was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Policy maps can include policers that specify the bandwidth limitations and the action to take if the limits are exceeded.
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:

- Filter-based classification counters are not supported.
- 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 redundancy

To display redundancy facility information, use the `show redundancy` command in privileged EXEC mode

```
show redundancy [{clients|config-sync|counters|history |{reload|reverse}}][slaves[slave-name]
{clients|counters}|states/switchover history [domain default]]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clients</td>
<td>(Optional) Displays information about the redundancy facility client.</td>
</tr>
<tr>
<td>config-sync</td>
<td></td>
</tr>
<tr>
<td>counters</td>
<td>(Optional) Displays information about the redundancy facility counter.</td>
</tr>
<tr>
<td>history</td>
<td>(Optional) Displays a log of past status and related information for the redundancy facility.</td>
</tr>
<tr>
<td>history reload</td>
<td>(Optional) Displays a log of past reload information for the redundancy facility.</td>
</tr>
<tr>
<td>history reverse</td>
<td>(Optional) Displays a reverse log of past status and related information for the redundancy facility.</td>
</tr>
<tr>
<td>slaves</td>
<td>(Optional) Displays all slaves in the redundancy facility.</td>
</tr>
<tr>
<td>slave-name</td>
<td>(Optional) The name of the redundancy facility slave to display specific information for. Enter additional keywords to display all clients or counters in the specified slave.</td>
</tr>
<tr>
<td>clients</td>
<td>Displays all redundancy facility clients in the specified slave.</td>
</tr>
<tr>
<td>counters</td>
<td>Displays all counters in the specified slave.</td>
</tr>
<tr>
<td>states</td>
<td>(Optional) Displays information about the redundancy facility state, such as disabled, initialization, standby or active.</td>
</tr>
<tr>
<td>switchover history</td>
<td>(Optional) Displays information about the redundancy facility switchover history.</td>
</tr>
<tr>
<td>domain default</td>
<td>(Optional) Displays the default domain as the domain to display switchover history for.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>Privileged EXEC (#)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

This example shows how to display information about the redundancy facility:

```
Device# show redundancy
Redundant System Information :
--------------------------------
Available system uptime = 6 days, 9 hours, 23 minutes
```
Switchovers system experienced = 0
Standby failures = 0
Last switchover reason = not known

Hardware Mode = Simplex
Configured Redundancy Mode = SSO
Operating Redundancy Mode = SSO
Maintenance Mode = Disabled
Communications = Down Reason: Simplex mode

Current Processor Information :
----------------------------------
Active Location = slot 1
Current Software state = ACTIVE
Uptime in current state = 6 days, 9 hours, 23 minutes
Image Version = Cisco IOS Software, IOS-XE Software, Catalyst 3
850 L3 Switch Software (CAT3850-UNIVERSALK9-M), Version 03.08.59.EMD EARLY DEPLOYMENT ENGINEERING NOVA WEEKLY BUILD, synced to DSGS_PI2_POSTPC_FLO_DSBU7_NG3K_1105
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Sun 16-S
Configuration register = 0x102

Peer (slot: 0) information is not available because it is in 'DISABLED' state

Device#

This example shows how to display redundancy facility client information:

Device# show redundancy clients
Group ID = 1

clientID = 20002 clientSeq = 4 EICORE HA Client
clientID = 24100 clientSeq = 5 WCM_CAPWAP
clientID = 24101 clientSeq = 6 WCM RRM HA
clientID = 24103 clientSeq = 8 WCM QOS HA
clientID = 24105 clientSeq = 10 WCM MOBILITY
clientID = 24106 clientSeq = 11 WCM DOT1X
clientID = 24107 clientSeq = 12 WCM APFROGUE
clientID = 24110 clientSeq = 15 WCM CIDS
clientID = 24111 clientSeq = 16 WCM_NETFLOW
clientID = 24112 clientSeq = 17 WCM_MCAST
clientID = 24120 clientSeq = 18 wcm_comet
clientID = 24001 clientSeq = 21 Table Manager Client
clientID = 20010 clientSeq = 24 SNMP SA HA Client
clientID = 20007 clientSeq = 27 Installer HA Client
clientID = 29 clientSeq = 60 Redundancy Mode RF
clientID = 139 clientSeq = 61 IFIndex
clientID = 3300 clientSeq = 62 Persistent Variable
clientID = 25 clientSeq = 68 CHKPT RF
clientID = 20005 clientSeq = 74 IIF-shim
clientID = 10001 clientSeq = 82 QEMU Platform RF

<output truncated>

The output displays the following information:

- clientID displays the client’s ID number.
- clientSeq displays the client’s notification sequence number.
- Current redundancy facility state.

This example shows how to display the redundancy facility counter information:
**Device# show redundancy counters**

Redundancy Facility OMs

- comm link up = 0
- comm link down = 0
- invalid client tx = 0
- null tx by client = 0
- tx failures = 0
- tx msg length invalid = 0
- client not rxing msgs = 0
- rx peer msg routing errors = 0
- null peer msg rx = 0
- errored peer msg rx = 0
- buffers tx = 0
- tx buffers unavailable = 0
- buffers rx = 0
- buffer release errors = 0
- duplicate client registers = 0
- failed to register client = 0
- Invalid client syncs = 0

**Device#**

This example shows how to display redundancy facility history information:

**Device# show redundancy history**

```
00:00:00 *my state = INITIALIZATION(2) peer state = DISABLED(1)
00:00:00 RF_EVENT_INITIALIZATION(524) op=0 rc=0
00:00:00 *my state = NEGOTIATION(3) peer state = DISABLED(1)
00:00:01 client added: Table Manager Client(24001) seq=21
00:00:01 client added: SNMP SA HA Client(20010) seq=24
00:00:06 client added: WCM_CAPWAP(24100) seq=5
00:00:06 client added: WCM QOS HA(24103) seq=8
00:00:07 client added: WCM_DOT1X(24106) seq=11
00:00:07 client added: EICORE HA Client(20002) seq=4
00:00:09 client added: WCM_MOBILITY(24105) seq=10
00:00:09 client added: WCM_NETFLOW(24111) seq=16
00:00:09 client added: WCM_APFROGUE(24107) seq=12
00:00:09 client added: WCM_RRM HA(24101) seq=6
00:00:09 client added: WCM_MCAST(24112) seq=17
00:00:09 client added: WCM_CID(24110) seq=15
00:00:09 client added: wcm_comet(24120) seq=18
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) First Slave(0) op=0 rc=0
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) Slave(6107) op=0 rc=0
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) Slave(6109) op=0 rc=0
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) Slave(6128) op=0 rc=0
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) Slave(8987) op=0 rc=0
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) Slave(8897) op=0 rc=0
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) Slave(8898) op=0 rc=0
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) Slave(8901) op=0 rc=0
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) Slave(8902) op=0 rc=0
00:00:22 RF_EVENT_SLAVE_STATUS_DONE(523) First Slave(0) op=405 rc=0
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) Redundancy Mode RF(29) op=0 rc=0
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) IfIndex(139) op=0 rc=0
```

<output truncated>

This example shows how to display information about the redundancy facility slaves:

**Device# show redundancy slaves**

Group ID = 1
Slave/Process ID = 6107 Slave Name = [installer]
This example shows how to display information about the redundancy facility state:

Device# show redundancy states
  my state = 13 -ACTIVE
  peer state = 1 -DISABLED
    Mode = Simplex
    Unit ID = 1

Redundancy Mode (Operational) = SSO
Redundancy Mode (Configured) = SSO
  Redundancy State = Non Redundant
    Manual Swact = disabled (system is simplex (no peer unit))

Communications = Down Reason: Simplex mode

  client count = 75
  client_notification_TMR = 360000 milliseconds
    keep_alive TMR = 9000 milliseconds
      keep_alive count = 0
      keep_alive threshold = 18
        RF debug mask = 0

Device#
show remote-lan all

To view the detailed output of all RLANs, use the `show remote-lan all` command.

```
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

<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>

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
```

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>Global configuration</td>
</tr>
<tr>
<td>Command History</td>
<td>Release</td>
</tr>
<tr>
<td></td>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
</tr>
</tbody>
</table>

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
Webauth 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**

This command was introduced.

Cisco IOS XE Gibraltar 16.10.1

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_pp1
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
```
<table>
<thead>
<tr>
<th>DHCP Required</th>
<th>Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP Server</td>
<td>Not Configured</td>
</tr>
<tr>
<td>Accounting List</td>
<td>Not Configured</td>
</tr>
</tbody>
</table>
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**

<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>

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

<table>
<thead>
<tr>
<th>Profile Name</th>
<th>Description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>rlan_named_pp1</td>
<td>Testing RLAN policy profile</td>
<td>Enabled</td>
</tr>
</tbody>
</table>
```
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**

<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>

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 ssh

To see the SSH connection status, use the `show ssh` command.

```
show ssh {connection-number | {vty connection-number }}
```

**Syntax Description**

- `connection-number`  SSH connection number. Valid range is 0 to 530.

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to see the SSH connection status:

```
Device# show ssh connection-number
```
show tech wireless client

To view wireless client related information, use show tech wireless client command.

show tech wireless client { mac-address | | [ append | begin | count | exclude | format | include | redirect | section | tee ] }

Syntax Description

- **mac-address**  Displays information for a particular client
- **append**  Appends redirected output to a URL
- **begin**  Displays lines that being with the entered regular expression
- **count**  Displays the number of lines matching the entered regular expression
- **exclude**  Excludes the lines matching the entered regular expression
- **format**  Formats the output using the specified specifications file
- **include**  Includes the lines matching the entered regular expression
- **redirect**  Redirects output to a URL
- **section**  Filters a section of the output
- **tee**  Copies output to a URL

Command Modes

- User EXEC (>
- Privileged EXEC (#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.111.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

The following example shows how to view information about wireless clients:

ewlcdoc-16.10.1#show tech wireless client

------------------showwirelessstatsclientsummary------------------
Number of Local Clients: 0
Number of Excluded Clients: 0

------------------------------showwirelessclientsummary------------------
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 dB
WLAN Configuration Information
WLAN Profile Name 11k Neighbor Report 11v BSS Transition

---------- show wireless client calls active ----------
Number of Active TSPEC calls on 802.11a and 802.11b/g : 0
Number of Active SIP calls on 802.11a and 802.11b/g : 0
---------- 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 Username

---------- show wireless exclusionlist ----------
---------- show wireless country configured ----------
Configured Country......................... US - United States
Configured Country Codes
US - United States 802.11a Indoor/,Outdoor/ 802.11b Indoor/,Outdoor 802.11g Indoor/,Outdoor
show wireless tag rf summary

Number of RF Tags: 2
RF tag name Description

xyz-rf  xyz-rf
default-rf-tag default RF tag

show wireless wgb summary

Number of WGBs: 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 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
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
show tech wireless client

Create Ack 0/0
Modify Ack 0/0
Delete Ack 0/0
NACK Notify 0/0
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>AP Name</th>
<th>Retransmit Interval</th>
<th>Retransmit Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>TSIM_AP-2</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>TSIM_AP-3</td>
<td>3</td>
<td>5</td>
</tr>
</tbody>
</table>

*** show ap dot11 24ghz cleanair air-quality summary ***

\[AQ = \text{Air Quality} \quad \text{DFS = Dynamic Frequency Selection}\]

*** show ap dot11 24ghz cleanair air-quality worst ***

AQ = Air Quality
DFS = Dynamic Frequency Selection

*** 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 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
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.

**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 Gibraltar 16.10.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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
```

Cisco Catalyst 9800 Series Wireless Controller Command Reference, Cisco IOS XE Gibraltar 16.10.x
show tech-support wireless ap

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
show tech-support wireless ap

------------ 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
- 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

<table>
<thead>
<tr>
<th>Controller name</th>
<th>Controller IP</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
------------------ 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
- Update Contribution Interference: Enable
- Update Contribution Load: Disable
- Update Contribution 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

<table>
<thead>
<tr>
<th>Base MAC</th>
<th>Ethernet MAC</th>
<th>AP Name</th>
<th>IP Address</th>
<th>Status</th>
<th>Last Failure Type</th>
<th>Last Disconnect Reason</th>
</tr>
</thead>
</table>

show ap rf-profile summary

Number of RF-profiles: 6

<table>
<thead>
<tr>
<th>RF Profile Name</th>
<th>Band</th>
<th>Description</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low_Client_Density_rf_5gh</td>
<td>5 GHz</td>
<td>pre configured Low Client Density rf</td>
<td>Up</td>
</tr>
<tr>
<td>High_Client_Density_rf_5gh</td>
<td>5 GHz</td>
<td>pre configured High Client Density r</td>
<td>Up</td>
</tr>
<tr>
<td>Low_Client_Density_rf_24gh</td>
<td>2.4 GHz</td>
<td>pre configured Low Client Density rf</td>
<td>Up</td>
</tr>
<tr>
<td>High_Client_Density_rf_24gh</td>
<td>2.4 GHz</td>
<td>pre configured High Client Density r</td>
<td>Up</td>
</tr>
<tr>
<td>Typical_Client_Density_rf_5gh</td>
<td>5 GHz</td>
<td>pre configured Typical Density rfpro Up</td>
<td></td>
</tr>
<tr>
<td>Typical_Client_Density_rf_24gh</td>
<td>2.4 GHz</td>
<td>pre configured Typical Client Densit Up</td>
<td></td>
</tr>
</tbody>
</table>

show ap slots

show ap summary

Number of APs: 0
show tech-support wireless ap

------------------ 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 tech-support wireless ap

------------------ 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**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>mac-address</strong> Client MAC address.</td>
<td></td>
</tr>
</tbody>
</table>

**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>

**Usage Guidelines**

The output of the following commands are displayed as part of the `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

**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

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>AP Name</th>
<th>WLAN UpTime(secs)</th>
<th>Rx Pkts</th>
<th>Tx Pkts</th>
<th>RSSI</th>
<th>SNR</th>
<th>Data Retries</th>
</tr>
</thead>
<tbody>
<tr>
<td>--------------</td>
<td>---------</td>
<td>-------------------</td>
<td>---------</td>
<td>---------</td>
<td>------</td>
<td>-----</td>
<td>--------------</td>
</tr>
</tbody>
</table>

------------------ 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

<table>
<thead>
<tr>
<th>Type</th>
<th>Station</th>
<th>Entry Lifetime</th>
<th>VLAN Override</th>
<th>IP Override</th>
<th>Audit-Session-Id</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>RF tag name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default-rf-tag</td>
<td>default RF tag</td>
</tr>
</tbody>
</table>

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
  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 -------------------

<table>
<thead>
<tr>
<th>Vlan</th>
<th>pal_if_hdl</th>
<th>mac</th>
<th>Input Uidb</th>
<th>Output Uidb</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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**

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

**Command Default**

| Command Default | None |

**Command Modes**

| 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>

**Usage Guidelines**

This command is available only on the platforms that have CPP datapath architecture, such as Cisco vEWLC, Cisco 9540 WLC, and Cisco 9880 WLC.

The output of the following commands are displayed as part of show tech-support wireless datapath command:

- 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
In the presence of a 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 dataphath statistics drop
- show platform hardware chassis standby qfp feature wireless capwap dataphath statistics fragmentation
- show platform hardware chassis standby qfp feature wireless capwap dataphath 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
------------------

+-------------------------------------------------------------------------+
<table>
<thead>
<tr>
<th>Global Drop Stats</th>
<th>Packets</th>
<th>Octets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled</td>
<td>22230</td>
<td>2045194</td>
</tr>
<tr>
<td>InvL2Hdr</td>
<td>4765368</td>
<td>744492240</td>
</tr>
<tr>
<td>Ipv4NoAdj</td>
<td>6</td>
<td>736</td>
</tr>
<tr>
<td>Ipv4NoRoute</td>
<td>18</td>
<td>2358</td>
</tr>
<tr>
<td>Ipv6mNoRoute</td>
<td>3</td>
<td>270</td>
</tr>
<tr>
<td>SWPortDrop</td>
<td>14432</td>
<td>2886027</td>
</tr>
<tr>
<td>SWPortSrcFilter</td>
<td>53265</td>
<td>53992718</td>
</tr>
<tr>
<td>SWPortStpState</td>
<td>42041</td>
<td>3269790</td>
</tr>
<tr>
<td>SWPortVlanNotCfg</td>
<td>5515542</td>
<td>674079804</td>
</tr>
<tr>
<td>SwitchL2m</td>
<td>78</td>
<td>10062</td>
</tr>
<tr>
<td>SwitchL2mIGMP</td>
<td>18866</td>
<td>1283348</td>
</tr>
<tr>
<td>SwitchL2mUnconfigWireless</td>
<td>78</td>
<td>11622</td>
</tr>
<tr>
<td>WlsCapwapNoTunnel</td>
<td>3</td>
<td>627</td>
</tr>
</tbody>
</table>

------------------ 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_RFFID  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_CLEAN  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
------------------

Global Per Cause Statistics
```
Number of punt causes = 136

<table>
<thead>
<tr>
<th>Counter ID</th>
<th>Punt Cause Name</th>
<th>Packets Received</th>
<th>Packets Transmitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>000</td>
<td>Reserved</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>001</td>
<td>MPLS ICMP Can't Fragment</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>002</td>
<td>IPv4 Options</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>003</td>
<td>Layer2 control and legacy</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>004</td>
<td>PPP Control</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>005</td>
<td>CLNS IS-IS Control</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>006</td>
<td>HDLC keepalives</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>007</td>
<td>ARP request or response</td>
<td>2687</td>
<td>2687</td>
</tr>
<tr>
<td>008</td>
<td>Reverse ARP request or response</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>009</td>
<td>Frame-relay LMI Control</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>010</td>
<td>Incomplete adjacency</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>011</td>
<td>For-us data</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>012</td>
<td>Mcast Directly Connected Source</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>013</td>
<td>Mcast IPv4 Options data packet</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>014</td>
<td>Skip egress processing</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>015</td>
<td>MPLS TTL expired</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>016</td>
<td>MPLS Reserved label (ie: 0-15)</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>017</td>
<td>IPv6 Bad hop limit</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>018</td>
<td>IPv6 Hop-by-hop Options</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>019</td>
<td>Mcast Internal Copy</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>020</td>
<td>Generic QFP generated packet</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>021</td>
<td>RP&lt;-&gt;QFP keepalive</td>
<td>46691</td>
<td>46691</td>
</tr>
<tr>
<td>022</td>
<td>QFP Fwall generated packet</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>023</td>
<td>Mcast IGMP Unroutable</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>024</td>
<td>Glean adjacency</td>
<td>2557</td>
<td>2556</td>
</tr>
<tr>
<td>025</td>
<td>Mcast PIM signaling</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>026</td>
<td>QFP ICMP generated packet</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>027</td>
<td>Subscriber session control</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Count</td>
<td>Count</td>
</tr>
<tr>
<td>---</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------</td>
<td>-------</td>
</tr>
<tr>
<td>028</td>
<td>Subscriber data switching back</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>029</td>
<td>RP handled ICMP</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>030</td>
<td>RP injected For-us data</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>031</td>
<td>Punt adjacency</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>032</td>
<td>SBC RTP DTMF</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>033</td>
<td>Pseudowire VCCV control channel</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>034</td>
<td>Generic QFP generated packet (keep GPM)</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>035</td>
<td>Ethernet slow protocol (ie: LACP, OAM)</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>036</td>
<td>Ethernet OAM Loopback</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>037</td>
<td>UNUSED</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>038</td>
<td>SPA IPC packet</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>039</td>
<td>Punt and replicate</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>040</td>
<td>PPPoE control</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>041</td>
<td>PPPoE session</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>042</td>
<td>L2TP control</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>043</td>
<td>IP Subscriber control (ie: FSOL, keepali)</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>044</td>
<td>L2TP session</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>045</td>
<td>BFD control</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>046</td>
<td>MVPN non-RPF signaling packet</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>047</td>
<td>MVPN PIM signalling packet</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>048</td>
<td>Mcast punt to RP</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>049</td>
<td>SBC generated packet</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>050</td>
<td>IPV6 packet</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>051</td>
<td>DMVPN NHRP redirect</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>052</td>
<td>FFR monitored prefix logging</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>053</td>
<td>FFR top talkers logging</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>054</td>
<td>FFR top talkers application logging</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>055</td>
<td>For-us control</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>056</td>
<td>RP injected for-us control</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>057</td>
<td>QFP VTCP generated packet</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>058</td>
<td>Layer2 bridge domain data packet</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>059</td>
<td>QFP Stile generated packet</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>060</td>
<td>IP subnet or broadcast packet</td>
<td>167</td>
<td>167</td>
</tr>
<tr>
<td>061</td>
<td>Ethernet CFM packet</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>062</td>
<td>Ethernet CFM notify packet</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>063</td>
<td>LISP LSB NOTIFICATION</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>064</td>
<td>Service Engine packet</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>065</td>
<td>L2BD Control packet from FIA</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>066</td>
<td>L2BD Control Message from CPP</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>067</td>
<td>MFR_LIP_CONTROL</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>068</td>
<td>Media Monitoring record punted from CPP</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>069</td>
<td>OTV Control packet</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>070</td>
<td>OTV ARP packet</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>071</td>
<td>REP control</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>072</td>
<td>IP MTU EXCEPTION</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>073</td>
<td>STP BPDU's</td>
<td>186832</td>
<td>186832</td>
</tr>
<tr>
<td>074</td>
<td>ACL log</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>075</td>
<td>EPC</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>076</td>
<td>Lisp Dynamic eid</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>077</td>
<td>L2 Control packet</td>
<td>122389</td>
<td>122389</td>
</tr>
<tr>
<td>078</td>
<td>WAAS CPP to CPP punt</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>079</td>
<td>dhcp snoop</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>080</td>
<td>Metric Mediation Agent record punted from</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>081</td>
<td>IPv6 DMVPN NHRP redirect</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>082</td>
<td>Ethernet CFM packet from core</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>083</td>
<td>Ethernet CFM punt fwd packet</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>084</td>
<td>PTP punt fwd packet</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>085</td>
<td>ISDN D-Channel raw packet</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>086</td>
<td>Service controller SCG punt pkt</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>087</td>
<td>IPv6 FHS SG dropped packet</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>088</td>
<td>IPv6 FHS Data glean packet</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>089</td>
<td>SBC DSP pkts</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>090</td>
<td>Raw Socket Data packet</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>091</td>
<td>SSLVPN session control</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
show tech-support wireless datapath

```
  092  ICMP unreachables 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 packet 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
```
<table>
<thead>
<tr>
<th>Counter ID</th>
<th>Inject Cause Name</th>
<th>Packets Received</th>
<th>Packets Transmitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>000</td>
<td>RESERVED</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>001</td>
<td>L2 control/legacy</td>
<td>3115</td>
<td>3115</td>
</tr>
<tr>
<td>002</td>
<td>QFP destination lookup</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>003</td>
<td>QFP IPv4/v6 nexthop lookup</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>004</td>
<td>QFP generated packet</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>005</td>
<td>QFP &lt;-&gt;RP keepalive</td>
<td>46691</td>
<td>0</td>
</tr>
<tr>
<td>006</td>
<td>QFP Fwall generated packet</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>007</td>
<td>QFP adjacency-id lookup</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>008</td>
<td>Mcast specific inject packet</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>009</td>
<td>QFP ICMP generated packet</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>010</td>
<td>QFP/RP-&gt;QFP Subscriber data packet</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>011</td>
<td>SBC DTMF</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>012</td>
<td>ARP request or response</td>
<td>3637</td>
<td>3637</td>
</tr>
<tr>
<td>013</td>
<td>Ethernet OAM loopback packet</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>No.</td>
<td>Description</td>
<td>Value 1</td>
<td>Value 2</td>
</tr>
<tr>
<td>-----</td>
<td>------------------------------------------------------------------------------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>014</td>
<td>UNUSED</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>015</td>
<td>PPPoE discovery packet</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>016</td>
<td>PPPoE session packet</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>017</td>
<td>QFP inject for pp_index lookup</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>018</td>
<td>QFP inject replicate</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>019</td>
<td>QFP inject PIT lookup</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>020</td>
<td>SBC generated packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>021</td>
<td>QFP VTCP generated packet</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>022</td>
<td>QFP Stile generated packet</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>023</td>
<td>Service Engine generated packet</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>024</td>
<td>Layer2 frame to EFP</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>025</td>
<td>Layer2 frame to BD</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>026</td>
<td>QfP Asym Routing redirected pkt</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>027</td>
<td>Compressed packet from WAAS</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>028</td>
<td>Media (e.g. voice) associated with a ses</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>029</td>
<td>service controller scg packet</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>030</td>
<td>Packet for 14 port Serial IM</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>031</td>
<td>Subscriber generated TCP reset packet</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>032</td>
<td>Layer2 frame to INPUT EFP</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>033</td>
<td>SSLVPN inject control</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>034</td>
<td>injected packet from UTD SP</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>035</td>
<td>injected packet from DPSS SN</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>036</td>
<td>injected packet by AppNav vPath</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>037</td>
<td>Uncompressed packet from WAAS</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>038</td>
<td>Autonomic Network Channel Discovery pack</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>039</td>
<td>Cable Bundle Flood Inject</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>040</td>
<td>Cable L2 unicast inject</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>041</td>
<td>downstream jib packet</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>042</td>
<td>switch port layer 2 control packet</td>
<td>6254</td>
<td>6253</td>
</tr>
<tr>
<td>043</td>
<td>Applications Injecting Pkts using LFTS</td>
<td>303874</td>
<td>303269</td>
</tr>
<tr>
<td>044</td>
<td>Enhanced ping and traceroute</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>045</td>
<td>Applications Injecting packets with SGT</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Show Commands

show tech-support wireless datapath

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 cpp_if_hdl pal_if_hdl in_uidb out_uidb
--------------------------------------------------------------------------------------------------------------------
WLAN-IF-0x00f0400001 0X74 0XF0400001 0X1768E 0X1768C
att
WLAN-IF-0x00f0400002 0X78 0XF0400002 0X1768A 0X17688
verizon

------------------ show platform software bssid chassis active F0 statistics
------------------

Bssid Counters (Success/Failure)
-----------------------------------
Create 0/0
Delete 0/0
HW Create 0/0

Cisco Catalyst 9800 Series Wireless Controller Command Reference, Cisco IOS XE Gibraltar 16.10.x
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 statistics --------------------

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
### Show Commands

```plaintext
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 ---------------

<table>
<thead>
<tr>
<th>Tun</th>
<th>Type</th>
<th>Pal_if_hdl</th>
<th>Ap Mac</th>
<th>Source IP</th>
<th>Destination IP</th>
<th>Destination Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>0X108</td>
<td>DATA</td>
<td>0X90000042</td>
<td>00a8.2200.0200</td>
<td>78.1.1.7</td>
<td>78.1.50.1</td>
<td>52345</td>
</tr>
<tr>
<td>0X10B</td>
<td>MOBILITY</td>
<td>0XA0000002</td>
<td>0000.0000.0000</td>
<td>78.1.1.7</td>
<td>78.1.1.23</td>
<td>16667</td>
</tr>
<tr>
<td>0X10C</td>
<td>MOBILITY</td>
<td>0XA0000003</td>
<td>0000.0000.0000</td>
<td>78.1.1.7</td>
<td>78.1.1.24</td>
<td>16667</td>
</tr>
<tr>
<td>0X10D</td>
<td>MOBILITY</td>
<td>0XA0000004</td>
<td>0000.0000.0000</td>
<td>78.1.1.7</td>
<td>78.1.1.25</td>
<td>16667</td>
</tr>
</tbody>
</table>

------------------ show platform hardware chassis active qfp feature wireless capwap
data path summary ---------------

<table>
<thead>
<tr>
<th>Vrf</th>
<th>Source Port</th>
<th>Destination IP</th>
<th>Dst Port</th>
<th>Input Uidb</th>
<th>Output Uidb</th>
<th>Instance Id</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>16667</td>
<td>78.1.1.25</td>
<td>16667</td>
<td>95733</td>
<td>95731</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>5247</td>
<td>78.1.50.1</td>
<td>52345</td>
<td>95738</td>
<td>95736</td>
<td>3</td>
</tr>
<tr>
<td>0</td>
<td>16667</td>
<td>78.1.1.24</td>
<td>16667</td>
<td>95734</td>
<td>95732</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>16667</td>
<td>78.1.1.23</td>
<td>16667</td>
<td>95735</td>
<td>95733</td>
<td>0</td>
</tr>
</tbody>
</table>

------------------ show platform hardware chassis active qfp feature wireless capwap
data path statistics drop ---------------

<table>
<thead>
<tr>
<th>Drop Cause</th>
<th>Packets</th>
<th>Octets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wls Capwap unsupported link type Error</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Wls Capwap invalid tunnel Error</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Wls Capwap input config missing Error</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Wls Capwap invalid TPID Error</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Wls Capwap ingress parsing Error</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```
Wls Capwap invalid FC subtype Error  0
Wls Capwap SNAP Invalid HLEN Error  0
Wls Client V6 Max Address Error  0

------------------ show platform hardware chassis active qfp feature wireless capwap datapath
statistics fragmentation ------------------

CPP Wireless Fragmentation stats:

<table>
<thead>
<tr>
<th>Description</th>
<th>Packet Count</th>
<th>Octet Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capwap Packets to be Fragmented (RX)</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Capwap Fragments to be Recycled</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Capwap Fragments Recycled (TX)</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Error: Original Packet Too Big</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Error: CAPWAP MTU Not Valid</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Error: Recycle Queue Full</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Error: Recycle Queue Not Valid</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Error: GFP Memory Init Failure</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Error: Multipass Requeue Failure</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

------------------ show platform hardware chassis active qfp feature wireless capwap datapath
statistics reassembly ------------------

CPP Wireless Reassembly Memory stats:

<table>
<thead>
<tr>
<th>Description</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Free info chunk</td>
<td>32768</td>
</tr>
<tr>
<td>Allocated info chunks</td>
<td>32768</td>
</tr>
<tr>
<td>Free fragment chunks</td>
<td>131072</td>
</tr>
<tr>
<td>Allocated fragment chunks</td>
<td>131072</td>
</tr>
</tbody>
</table>

CPP Wireless Reassembly Packet stats: (outstanding pkt_cnt 0)

<table>
<thead>
<tr>
<th>Description</th>
<th>Packet Count</th>
<th>Octet Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capwap Reassembled Packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Capwap Fragments Received</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Capwap Fragments Consumed (Saved)</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Capwap Fragments Dropped</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Capwap Reassembly Timeouts</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Error - Early-drop fragments</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Error - Invalid packet size</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Error - Fragment size too big</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Error - Too many fragments</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Error - Overlap offset fragments</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Error - Duplicated fragments</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Error - Allocate info chunk memory</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Error - Allocate frag chunk memory</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Error - Hash bucket threshold</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Error - Cannot save and gather pkts</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Error - Get recycle reass_info NULL</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Error - BQS memory alloc NULL</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Error - BQS memory free NULL</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
DEBUG - # of lock sync acquired  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)

<table>
<thead>
<tr>
<th>Action</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create</td>
<td>847/0</td>
</tr>
<tr>
<td>Delete</td>
<td>424/0</td>
</tr>
<tr>
<td>HW Create</td>
<td>425/0</td>
</tr>
<tr>
<td>HW Modify</td>
<td>422/0</td>
</tr>
<tr>
<td>HW Delete</td>
<td>424/0</td>
</tr>
<tr>
<td>Create Ack</td>
<td>425/0</td>
</tr>
<tr>
<td>Modify Ack</td>
<td>422/0</td>
</tr>
<tr>
<td>Delete Ack</td>
<td>424/0</td>
</tr>
<tr>
<td>Ack Ack Notify</td>
<td>1271/0</td>
</tr>
<tr>
<td>Nack Notify</td>
<td>0/0</td>
</tr>
<tr>
<td>HA Seq GET</td>
<td>782/0</td>
</tr>
<tr>
<td>HA Seq SET</td>
<td>0/0</td>
</tr>
<tr>
<td>HA Seq Crypto GET</td>
<td>1542/0</td>
</tr>
<tr>
<td>HA Seq Crypto SET</td>
<td>0/0</td>
</tr>
<tr>
<td>HA Seq Crypto Callback</td>
<td>1542/0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Action</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>HA Seq last Responded</td>
<td>0</td>
</tr>
<tr>
<td>HA Seq Pending</td>
<td>0</td>
</tr>
<tr>
<td>HA Seq Outstanding cb</td>
<td>0</td>
</tr>
<tr>
<td>Total DTLS CTX count</td>
<td>1</td>
</tr>
</tbody>
</table>

---------- show platform software dtls chassis active F0 ----------

Forwarding Manager DTLS Session Summary

<table>
<thead>
<tr>
<th>Session ID</th>
<th>Type</th>
<th>Peer IP</th>
<th>Port</th>
<th>AOM ID</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0300000000000001</td>
<td>AP Control</td>
<td>78.1.50.1</td>
<td>52345</td>
<td>3270</td>
<td>Done</td>
</tr>
</tbody>
</table>

---------- 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

<table>
<thead>
<tr>
<th>Counter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create from fp</td>
<td>425</td>
</tr>
<tr>
<td>Modify from fp</td>
<td>422</td>
</tr>
<tr>
<td>Delete from fp</td>
<td>424</td>
</tr>
</tbody>
</table>
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 ------------------

<table>
<thead>
<tr>
<th>Session ID</th>
<th>CDH Handle</th>
<th>Session Type</th>
<th>Parent if-h</th>
<th>Instance id</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0300000000000001</td>
<td>0x00000000D902D9E0</td>
<td>AP Control</td>
<td>0</td>
<td>3</td>
</tr>
</tbody>
</table>

------------------ show platform hardware chassis active qfp feature wireless dtls datapath
summary ------------------

<table>
<thead>
<tr>
<th>Src IP</th>
<th>Dst IP</th>
<th>Src Port</th>
<th>Dst Port</th>
<th>Crypto HDL</th>
<th>Instance Id</th>
</tr>
</thead>
<tbody>
<tr>
<td>78.1.1.7</td>
<td>78.1.50.1</td>
<td>5246</td>
<td>52345</td>
<td>0xd902d9e0</td>
<td>3</td>
</tr>
</tbody>
</table>

------------------ show platform hardware chassis active qfp feature wireless dtls datapath
statistics ------------------

CPP Wireless DTLS Feature Stats

<table>
<thead>
<tr>
<th>Description</th>
<th>Packet Count</th>
<th>Octet Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>DTLS Packets To Encrypt</td>
<td>286494</td>
<td>8860778</td>
</tr>
<tr>
<td>DTLS Packets Encrypted</td>
<td>286494</td>
<td>35681366</td>
</tr>
<tr>
<td>DTLS Packets To Decrypt</td>
<td>286734</td>
<td>41001830</td>
</tr>
<tr>
<td>DTLS Packets Decrypted</td>
<td>286734</td>
<td>33401602</td>
</tr>
<tr>
<td>Skip Encryption - Handshake</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Skip Encryption - Not AppData</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Skip Encryption - No Hash Entry</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Skip Encryption - No Crypto Handle</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Skip Encryption - No DTLS header</td>
<td>563</td>
<td>76419</td>
</tr>
<tr>
<td>Skip Encryption - Requested by RP</td>
<td>16234</td>
<td>5042852</td>
</tr>
<tr>
<td>Skip Decryption - Handshake</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Skip Decryption - Not AppData</td>
<td>2949</td>
<td>996248</td>
</tr>
<tr>
<td>Skip Decryption - No Hash Entry</td>
<td>447</td>
<td>56474</td>
</tr>
<tr>
<td>Skip Decryption - No Crypto Handle</td>
<td>13024</td>
<td>3626640</td>
</tr>
<tr>
<td>Skip Decryption - No DTLS header</td>
<td>507</td>
<td>116600</td>
</tr>
<tr>
<td>Skip Decryption - Multiple Records</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Error - Encrypt Invalid Length</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Error - Encrypt Header Restore</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Error - DataEncrypt No Crypto Handle</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Error - DataEncrypt Header Restore</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Error - Decrypt Invalid Length</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Error - Decrypt Header Restore</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Error - DataDecrypt Zero Epoch</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
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 nack 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
### Mobility State Abbreviations:
- **UK**: UNKNOWN
- **IN**: INIT
- **LC**: LOCAL
- **AN**: ANCHOR
- **FR**: FOREIGN
- **MT**: MTE
- **IV**: INVALID

### Data Path Table

<table>
<thead>
<tr>
<th>VLAN</th>
<th>pal_if_hdl</th>
<th>MAC Address</th>
<th>Input Uidb</th>
<th>Output Uidb</th>
</tr>
</thead>
<tbody>
<tr>
<td>177</td>
<td>0xa0000001</td>
<td>0028.b122.0001</td>
<td>95744</td>
<td>95742</td>
</tr>
</tbody>
</table>

### Data Path Statistic Drop

<table>
<thead>
<tr>
<th>Drop Cause</th>
<th>Packets</th>
<th>Octets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wls Client V6 Max Address Error</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Wls Client IPGlean Counter Index Error</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Wls Client IPGlean Counter Unchanged Error</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Wls Client IPGlean alloc no memory Error</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Wls Client invalid punt packet error</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Wls Client input subblock missing error</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Wls Client input config missing</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Wls Client global mac address fetch error</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Wls Client header add error</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Wls Client IP entry theft error</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Wls Client IPSG input subblock missing error</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Wls Client DOT1Q Hdr add anchor error</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Wls Client DOT1Q Hdr add anchor avc error</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Wls Client Guest Foreign Multicast error</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
### CPP Wireless IPv6 Data Gleaning Table:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>VLAN</th>
<th>uIDB</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### CPP Wireless IPSG CPP-client Statistics

<table>
<thead>
<tr>
<th>Counter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total IPv4 Address Count</td>
<td>1</td>
</tr>
<tr>
<td>Total IPv6 Address Count</td>
<td>0</td>
</tr>
<tr>
<td>IPv4 Entry Add Success</td>
<td>56</td>
</tr>
<tr>
<td>IPv4 Entry Add Fail</td>
<td>0</td>
</tr>
<tr>
<td>IPv4 Entry Delete Success</td>
<td>55</td>
</tr>
<tr>
<td>IPv4 Entry Delete Fail</td>
<td>0</td>
</tr>
<tr>
<td>IPv6 Entry Add Success</td>
<td>0</td>
</tr>
<tr>
<td>IPv6 Entry Add Fail</td>
<td>0</td>
</tr>
<tr>
<td>IPv6 Entry Delete Success</td>
<td>0</td>
</tr>
<tr>
<td>IPv6 Entry Delete Fail</td>
<td>0</td>
</tr>
<tr>
<td>IP Entry Override</td>
<td>0</td>
</tr>
<tr>
<td>IP Entry Add Req Skip</td>
<td>0</td>
</tr>
<tr>
<td>Data Glean Memory Req Recv</td>
<td>0</td>
</tr>
<tr>
<td>Data Glean Memory Req Fail</td>
<td>0</td>
</tr>
<tr>
<td>Data Glean Memory Reg Send</td>
<td>0</td>
</tr>
<tr>
<td>Data Glean Memory Ret Recv</td>
<td>0</td>
</tr>
<tr>
<td>Data Glean Memory Ret Send</td>
<td>0</td>
</tr>
<tr>
<td>Data Glean Entry Send</td>
<td>0</td>
</tr>
<tr>
<td>IPSG Subblock Allocate</td>
<td>0</td>
</tr>
<tr>
<td>IPSG Subblock Allocate Fail</td>
<td>0</td>
</tr>
<tr>
<td>IPSG Subblock Free</td>
<td>0</td>
</tr>
<tr>
<td>IPSG Subblock Free Fail</td>
<td>0</td>
</tr>
<tr>
<td>IPSG FIA Enable</td>
<td>0</td>
</tr>
<tr>
<td>IPSG FIA Enable Fail</td>
<td>0</td>
</tr>
<tr>
<td>IPSG FIA Disable</td>
<td>0</td>
</tr>
<tr>
<td>IPSG FIA Disable Fail</td>
<td>0</td>
</tr>
<tr>
<td>IPSG Feature Enable</td>
<td>0</td>
</tr>
<tr>
<td>IPSG Feature Enable Fail</td>
<td>0</td>
</tr>
<tr>
<td>IPSG Feature Disable</td>
<td>0</td>
</tr>
<tr>
<td>IPSG Feature Disable Fail</td>
<td>0</td>
</tr>
</tbody>
</table>

### CPP Wireless IPSG Table Summary

Total number of address entries: 1

<table>
<thead>
<tr>
<th>IP Address</th>
<th>VLAN</th>
<th>uIDB</th>
</tr>
</thead>
<tbody>
<tr>
<td>177.1.0.7</td>
<td>177</td>
<td>95744</td>
</tr>
</tbody>
</table>

------------------ show platform hardware chassis active qfp feature wireless ipsg datapath

------------------ show platform hardware chassis active qfp feature wireless ipsg cpp-client

------------------ show platform hardware chassis active qfp feature wireless ipsg cpp-client
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

CPP Wireless IPSG IPv4 Table:
IP Address  VLAN  uIDB  Interface
---------------------------------------- ---- ------ -------------
177.1.0.7

CPP Wireless IPSG IPv6 Table:
IP Address  VLAN  uIDB  Interface
---------------------------------------- ---- ------ -------------

Wireless HALO Statistics
Rx Packet Count  0
Rx Packet Bytes  0

CPP Wireless FQDN Filter Info:
ID  Type  DSA_hdl  Redirect_IPv4  Virtual_IPv4
----  ------  ---------  ------------  ------------

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 tech-support wireless datapath

---

text

---

text
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**

<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>

**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.

**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>

**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
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 : 0
    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 : 0
  - Ok : 0
  - Deny - generic : 0
  - Client blacklisted : 0
  - Client limit reached : 0
  - Profile mismatch : 0
  - Deny - unknown reason : 0
- Request Received : 0
- Response Sent : 0
  - 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
- Unknown events : 0
- Event schedule errors : 0
- Internal errors : 0

------------------ show wireless stats mobility messages ------------------

MM datagram message statistics:
<table>
<thead>
<tr>
<th>Message Type</th>
<th>Built</th>
<th>Tx</th>
<th>Rx</th>
<th>Processed</th>
<th>Tx Error</th>
<th>Rx Error</th>
<th>Forwarded</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile Announce</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobile Announce Nak</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Cisco Catalyst 9800 Series Wireless Controller Command Reference, Cisco IOS XE Gibraltar 16.10.x
<table>
<thead>
<tr>
<th>Message Type</th>
<th>Built Tx</th>
<th>Rx</th>
<th>Processed Tx</th>
<th>Error Rx</th>
<th>Error Tx</th>
<th>Error Processed Tx</th>
<th>Forwarded</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static IP Mobile Annce</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Static IP Mobile Annce Resp</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Handoff</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Handoff End</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Handoff End Ack</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Anchor Req</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Anchor Grant</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Anchor Xfer</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Anchor Xfer Ack</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Export Anchor Req</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Export Anchor Resp</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>AAA Handoff</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>AAA Handoff Ack</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>IPv4 Addr Update</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>IPv4 Addr Update Ack</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>IPv6 ND Packet</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>IPv6 Addr Update</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>IPv6 Addr Update Ack</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Client Add</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Client Delete</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Keepalive Ctrl Req</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Keepalive Ctrl Resp</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>AP List Update</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Client Device Profile Info</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PMK Update</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PMK Delete</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PMK 11r Nonce Update</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Device cache Update</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>HA SSO Announce</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>HA SSO Announce Resp</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Cisco Catalyst 9800 Series Wireless Controller Command Reference, Cisco IOS XE Gibraltar 16.10.x
### MMIF IPC message statistics:

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Built</th>
<th>Tx</th>
<th>Rx</th>
<th>Processed</th>
<th>Tx Error</th>
<th>Rx Error</th>
<th>Drops</th>
<th>Allocs</th>
</tr>
</thead>
<tbody>
<tr>
<td>HA SSO Announce Resp</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Mobile Announce: 0 0 0 0 0 0 0 0
Mobile Announce Nak: 0 0 0 0 0 0 0 0
Static IP Mobile Annnc: 0 0 0 0 0 0 0 0
Static IP Mobile Annnc Rsp: 0 0 0 0 0 0 0 0
Handoff: 0 0 0 0 0 0 0 0
Handoff End: 0 0 0 0 0 0 0 0
Handoff End Ack: 0 0 0 0 0 0 0 0
Anchor Req: 0 0 0 0 0 0 0 0
Anchor Grant: 0 0 0 0 0 0 0 0
Anchor Xfer: 0 0 0 0 0 0 0 0
Anchor Xfer Ack: 0 0 0 0 0 0 0 0
Export Anchor Req: 0 0 0 0 0 0 0 0
Export Anchor Rsp: 0 0 0 0 0 0 0 0
AAA Handoff: 0 0 0 0 0 0 0 0
AAA Handoff Ack: 0 0 0 0 0 0 0 0
IPv4 Addr Update: 0 0 0 0 0 0 0 0
IPv4 Addr Update Ack: 0 0 0 0 0 0 0 0
IPv6 ND Packet: 0 0 0 0 0 0 0 0
IPv6 Addr Update: 0 0 0 0 0 0 0 0
IPv6 Addr Update Ack: 0 0 0 0 0 0 0 0
Client Add: 0 0 0 0 0 0 0 0
Client Delete: 0 0 0 0 0 0 0 0
Keepalive Ctrl Req: 0 0 0 0 0 0 0 0
Keepalive Ctrl Resp: 0 0 0 0 0 0 0 0
AP List Update: 0 0 0 0 0 0 0 0
Client Device Profile Info: 0 0 0 0 0 0 0 0
PMK Update: 0 0 0 0 0 0 0 0
PMK Delete 0 0 0 0 0 0 0 0
PMK 11r Nonce Update 0 0 0 0 0 0 0 0
Device cache Update 0
HA SSO Announce 0
HA SSO Announce Resp 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:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Public Ip</th>
<th>Group Name</th>
<th>Status</th>
<th>Multicast IPv4</th>
<th>PMTU</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.12.32.10</td>
<td>N/A</td>
<td>default</td>
<td>N/A</td>
<td>0.0.0.0</td>
<td>::</td>
</tr>
</tbody>
</table>

------------------ 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 ------------------

<table>
<thead>
<tr>
<th>Vrf</th>
<th>Src Port</th>
<th>Dst IP</th>
<th>Dsp Port</th>
<th>Input Uidb</th>
<th>Output Uidb</th>
<th>Instance Id</th>
</tr>
</thead>
<tbody>
<tr>
<td>---</td>
<td>--------</td>
<td>------</td>
<td>--------</td>
<td>----------</td>
<td>-------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>

------------------ show platform hardware chassis active qfp feature wireless dtls datapath
statistics -------------

CPP Wireless DTLS Feature Stats

<table>
<thead>
<tr>
<th>Description</th>
<th>Packet Count</th>
<th>Octet Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>DTLS Packets To Encrypt</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>DTLS Packets Encrypted</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>DTLS Packets To Decrypt</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>DTLS Packets Decrypted</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Skip Encryption - Handshake</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Skip Encryption - Not AppData</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Skip Encryption - No Hash Entry</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Skip Encryption - No Crypto Handle</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Skip Encryption - No DTLS header</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Skip Encryption - Requested by RP</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Skip Decryption - Handshake</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Skip Decryption - Not AppData</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Skip Decryption - No Hash Entry</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Skip Decryption - No Crypto Handle</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Skip Decryption - No DTLS header</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Skip Decryption - Multiple Records</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Error - Encrypt Invalid Length</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Error - Encrypt Header Restore</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Error - DataEncrypt No Crypto Handle</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Error - DataEncrypt Header Restore</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Error - Decrypt Invalid Length</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Error - Decrypt Header Restore</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Error - DataDecrypt Zero Epoch</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Error - DataDecrypt No Hash Entry</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Error - DataDecrypt No Crypto Handle</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Error - DataDecrypt Header Restore</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

------------------ show platform hardware chassis active qfp feature wireless dtls datapath
summary ------------------

<table>
<thead>
<tr>
<th>Src IP</th>
<th>Dst IP</th>
<th>Src Port</th>
<th>Dst Port</th>
<th>Crypto HDL</th>
<th>Instance Id</th>
</tr>
</thead>
<tbody>
<tr>
<td>------</td>
<td>------</td>
<td>--------</td>
<td>---------</td>
<td>------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>

------------------ 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

Cisco Catalyst 9800 Series Wireless Controller Command Reference, Cisco IOS XE Gibraltar 16.10.x
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/29184a6d15c1ba11acb2d0bd22eb6e36/0 created:33 destroyed:33
diff:0

Cisco Catalyst 9800 Series Wireless Controller Command Reference, Cisco IOS XE Gibraltar 16.10.x
Cisco Catalyst 9800 Series Wireless Controller Command Reference, Cisco IOS XE Gibraltar 16.10.x

Show Commands

show tech-support wireless mobility
```plaintext
--- show platform software memory mobilityd chassis active R0 brief ---

<table>
<thead>
<tr>
<th>module</th>
<th>allocated</th>
<th>requested</th>
<th>allocs</th>
<th>frees</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>620441</td>
<td>617113</td>
<td>233</td>
<td>25</td>
</tr>
<tr>
<td>unknown</td>
<td>198515</td>
<td>198435</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>chunk</td>
<td>139689</td>
<td>139209</td>
<td>30</td>
<td>0</td>
</tr>
<tr>
<td>eventutil</td>
<td>118939</td>
<td>118299</td>
<td>48</td>
<td>8</td>
</tr>
<tr>
<td>process</td>
<td>67642</td>
<td>67594</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>odm-db-ctx</td>
<td>29950</td>
<td>28430</td>
<td>100</td>
<td>5</td>
</tr>
<tr>
<td>uipeer</td>
<td>22672</td>
<td>22592</td>
<td>11</td>
<td>6</td>
</tr>
<tr>
<td>odm-ipc-ctx</td>
<td>20272</td>
<td>19984</td>
<td>18</td>
<td>0</td>
</tr>
<tr>
<td>unknown</td>
<td>18024</td>
<td>18008</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>odm-client-ctx</td>
<td>1872</td>
<td>1824</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>cdllib</td>
<td>1688</td>
<td>1672</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>trccfg</td>
<td>512</td>
<td>496</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>bidb</td>
<td>472</td>
<td>456</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>unknown</td>
<td>96</td>
<td>48</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>bcrdu_avl</td>
<td>72</td>
<td>56</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>orchestrator_main</td>
<td>26</td>
<td>10</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
```
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.

**Syntax Description**

```
show tech-support wireless radio
```

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>

**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 Rf1 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
show tech-support wireless radio

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

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 RM 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

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

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

<table>
<thead>
<tr>
<th>Controller name</th>
<th>Controller IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>ewlc-doc</td>
<td>9.12.32.10</td>
</tr>
</tbody>
</table>

------------------ 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

<table>
<thead>
<tr>
<th>Controller name</th>
<th>Controller IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>ewlc-doc</td>
<td>9.12.32.10</td>
</tr>
</tbody>
</table>

------------------ 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
show tech-support wireless radio

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
Show Commands

show tech-support wireless radio

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:
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
T1 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

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 tech-support wireless radio

------------- 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

<table>
<thead>
<tr>
<th>RF Profile Name</th>
<th>Band</th>
<th>Description</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low_Client_Density_rf_5gh</td>
<td>5 GHz</td>
<td>pre configured Low Client Density rf</td>
<td>Up</td>
</tr>
<tr>
<td>High_Client_Density_rf_5gh</td>
<td>5 GHz</td>
<td>pre configured High Client Density r</td>
<td>Up</td>
</tr>
<tr>
<td>Low_Client_Density_rf_24gh</td>
<td>2.4 GHz</td>
<td>pre configured Low Client Density rf</td>
<td>Up</td>
</tr>
<tr>
<td>High_Client_Density_rf_24gh</td>
<td>2.4 GHz</td>
<td>pre configured High Client Density r</td>
<td>Up</td>
</tr>
<tr>
<td>Typical_Client_Density_rf_5gh</td>
<td>5 GHz</td>
<td>pre configured Typical Density rfpro</td>
<td>Up</td>
</tr>
<tr>
<td>Typical_Client_Density_rf_24gh</td>
<td>2.4 GHz</td>
<td>pre configured Typical Client Densit</td>
<td>Up</td>
</tr>
</tbody>
</table>

------------- 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

<table>
<thead>
<tr>
<th>AP Name</th>
<th>MAC Address</th>
<th>Slot ID</th>
<th>Current-Band</th>
<th>COF %</th>
<th>Suggested Mode</th>
</tr>
</thead>
</table>

COF : Coverage Overlap Factor

------------- show wireless band-select -------------

  Band Select Probe Response : per WLAN enabling
  Cycle Count : 2
  Cycle Threshold (millsec) : 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 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**

<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>

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

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**

<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>

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>

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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
</tr>
</tbody>
</table>

This example shows how to view the Umbrella DNSCrypt details:

```
Device# show umbrella dnscrypt
DNSCrypt: Enabled

Certificate Update Status:
  Last Successful 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 :
  Client Secret Key Hash:
  Client Public key :
  NM key Hash :
```
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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>brief</td>
<td>(Optional) Displays one line for each VLAN with the VLAN name, status, and its ports.</td>
</tr>
<tr>
<td>group</td>
<td>(Optional) Displays information about VLAN groups.</td>
</tr>
<tr>
<td>id vlan-id</td>
<td>(Optional) Displays information about a single VLAN identified by the VLAN ID number. For <code>vlan-id</code>, the range is 1 to 4094.</td>
</tr>
<tr>
<td>mtu</td>
<td>(Optional) Displays a list of VLANs and the minimum and maximum transmission unit (MTU) sizes configured on ports in the VLAN.</td>
</tr>
<tr>
<td>name vlan-name</td>
<td>(Optional) Displays information about a single VLAN identified by the VLAN name. The VLAN name is an ASCII string from 1 to 32 characters.</td>
</tr>
<tr>
<td>remote-span</td>
<td>(Optional) Displays information about Remote SPAN (RSPAN) VLANs.</td>
</tr>
<tr>
<td>summary</td>
<td>(Optional) Displays VLAN summary information.</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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.
### show vlan

#### VLAN Name

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Name</th>
<th>Status</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>default</td>
<td>active</td>
<td>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</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Type</th>
<th>SAID</th>
<th>MTU</th>
<th>Parent</th>
<th>RingNo</th>
<th>BridgeNo</th>
<th>Stp</th>
<th>BrdgMode</th>
<th>Trans1</th>
<th>Trans2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enet</td>
<td>1000001</td>
<td>1500</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>enet</td>
<td>1000002</td>
<td>1500</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>40</td>
<td>enet</td>
<td>100040</td>
<td>1500</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>300</td>
<td>enet</td>
<td>100300</td>
<td>1500</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1002</td>
<td>fddi</td>
<td>101002</td>
<td>1500</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1003</td>
<td>tr</td>
<td>101003</td>
<td>1500</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1004</td>
<td>fddnet</td>
<td>101004</td>
<td>1500</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>iee</td>
<td>-</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1005</td>
<td>trnet</td>
<td>101005</td>
<td>1500</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>ibm</td>
<td>-</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2000</td>
<td>enet</td>
<td>102000</td>
<td>1500</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3000</td>
<td>enet</td>
<td>103000</td>
<td>1500</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

#### Remote SPAN VLANs

<table>
<thead>
<tr>
<th>VLAN1</th>
<th>VLAN2</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000</td>
<td>3000</td>
</tr>
</tbody>
</table>

#### Primary Secondary Type

<table>
<thead>
<tr>
<th>Primary</th>
<th>Secondary</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

### Table 15: show vlan Command Output Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>VLAN number.</td>
</tr>
<tr>
<td>Name</td>
<td>Name, if configured, of the VLAN.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the VLAN (active or suspend).</td>
</tr>
<tr>
<td>Ports</td>
<td>Ports that belong to the VLAN.</td>
</tr>
<tr>
<td>Type</td>
<td>Media type of the VLAN.</td>
</tr>
</tbody>
</table>
### Fields Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAID</td>
<td>Security association ID value for the VLAN.</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum transmission unit size for the VLAN.</td>
</tr>
<tr>
<td>Parent</td>
<td>Parent VLAN, if one exists.</td>
</tr>
<tr>
<td>RingNo</td>
<td>Ring number for the VLAN, if applicable.</td>
</tr>
<tr>
<td>BrdgNo</td>
<td>Bridge number for the VLAN, if applicable.</td>
</tr>
<tr>
<td>Stp</td>
<td>Spanning Tree Protocol type used on the VLAN.</td>
</tr>
<tr>
<td>BrdgMode</td>
<td>Bridging mode for this VLAN—possible values are source-route bridging (SRB) and source-route transparent (SRT); the default is SRB.</td>
</tr>
<tr>
<td>Trans1</td>
<td>Translation bridge 1.</td>
</tr>
<tr>
<td>Trans2</td>
<td>Translation bridge 2.</td>
</tr>
<tr>
<td>Remote SPAN VLANs</td>
<td>Identifies any RSPAN VLANs that have been configured.</td>
</tr>
</tbody>
</table>

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**
- **map-name** (Optional) Name of a specific VLAN access map.

**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 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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 name** *(Optional)* Displays filtering information for the specified VLAN access map.
- **vlan vlan-id** *(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 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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:

```
Device# show vlan group group-name group2
vlan group group1 :40-45
```

This example shows how to display number of users in each of the VLANs in a group:

```
Device# show vlan group group-name group2 user_count
VLAN : Count
----------------------
  40 : 5
  41 : 8
  42 : 12
  43 : 2
  44 : 9
  45 : 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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 (millisecc) : 200
Age Out Suppression (sec) : 20
Age Out Dual Band (sec) : 60
Client RSSI (dBm) : 80
```
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>device</td>
<td>Shows classified devices.</td>
</tr>
<tr>
<td>steering</td>
<td>Wireless client steering information</td>
</tr>
<tr>
<td>cache</td>
<td>Shows the cached classified device summary.</td>
</tr>
<tr>
<td>count</td>
<td>Shows the wireless device count.</td>
</tr>
<tr>
<td>summary</td>
<td>Shows the active classified device summary.</td>
</tr>
<tr>
<td>chassis-number</td>
<td>Chassis number. Valid range is 1–2.</td>
</tr>
<tr>
<td>active</td>
<td>Active instance.</td>
</tr>
<tr>
<td>standby</td>
<td>Standby instance.</td>
</tr>
<tr>
<td>R0</td>
<td>Route-Processor slot 0.</td>
</tr>
</tbody>
</table>

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**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**

- `mac-address` Client MAC address.
- `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**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to see detailed client information using its MAC address:

```
Device# show wireless client mac-address 98-C7-7B-09-EF-ED 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

- **mac-address**
  - 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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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-3b3b0.3d27da1e-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**

- `mac-address`: The client MAC address.
- `tclas`: Displays TCLAS and user priority-related information about a client.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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 DestPort 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 mobility history` command.

```
show wireless client mac-address mac-address mobility history
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>mac-address</code></td>
<td>MAC address of the client.</td>
</tr>
<tr>
<td><code>chassis-number</code></td>
<td>Chassis number as either 1 or 2.</td>
</tr>
<tr>
<td><code>active R0</code></td>
<td>Active instance of the client in Route-processor slot 0.</td>
</tr>
<tr>
<td><code>standby R0</code></td>
<td>Standby instance of the client in Route-processor slot 0.</td>
</tr>
<tr>
<td><code>events</code></td>
<td>Shows client FSM event history.</td>
</tr>
</tbody>
</table>

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**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 summary

To display a summary of active clients associated with the controller, use the `show wireless client summary` command in privileged EXEC mode.

```
Device# show wireless client summary
Number of Local Clients : 1

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>AP Name</th>
<th>WLAN State</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000.1515.000f</td>
<td>AP-2</td>
<td>1</td>
<td>11a</td>
</tr>
</tbody>
</table>
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No default behavior or values.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 (blacklisted).
**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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>3.2SE</td>
<td></td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOSXE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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.
(,-) = (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

802.11a :
Channels : 3 3 3 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 8 2 6 0 4 8 2 6 0 4 8 2 6 0 9 3 7 1 5

4.9GHz 802.11a :
Channels : 1 1 1 1 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
```

Cisco Catalyst 9800 Series Wireless Controller Command Reference, Cisco IOS XE Gibraltar 16.10.x
The following is sample output from the `show wireless country configured` command:

```
Device# show wireless country configured
Configured Country.............................: US - United States
Configured Country Codes
  US - United States : 802.11a Indoor,Outdoor/ 802.11b / 802.11g
```

The following is sample output from the `show wireless country supported tx-power` command:

```
Device# show wireless country supported tx-power
KEY: ##  = Tx Power in dBm.
   ##* = Channel supports radar detection .
        . = Channel is not legal in this country.
         (-) = Regulatory Domains allowed by this country.
         (-,-) = (indoor, outdoor) regulatory Domains allowed by this country.

-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-

802.11bg :
Channels : 1 1 1 1
           : 1 2 3 4 5 6 7 8 9 0 1 2 3 4
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-

(CE ,CE ) AE : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(CE ,CE ) AL : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(AR ,AR ) AP : 27 27 27 27 27 27 27 27 27 27 27 27 27 27
(E ,E ) AT : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(A NA ) AU : 27 27 27 27 27 27 27 27 27 27 27 27 27 27
(A ,E ) BA : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(E ,E ) BE : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(E ,E ) BG : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(E ,E ) BH : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-A ,A ) BO : 27 27 27 27 27 27 27 27 27 27 27 27 27 27
(-A ,AR ) BR : 27 27 27 27 27 27 27 27 27 27 27 27 27 27
(E ,E ) BY : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(E ,E ) CA : 27 27 27 27 27 27 27 27 27 27 27 27 27 27
(A ,ABN ) CA2 : 27 27 27 27 27 27 27 27 27 27 27 27 27 27
(-E ,E ) CH : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(AER ,AR ) CL : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-E ,E ) CM : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(CE ,CE ) CN : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(A ,AR ) CO : 27 27 27 27 27 27 27 27 27 27 27 27 27 27
(A ,AB ) CR : 27 27 27 27 27 27 27 27 27 27 27 27 27 27
(-E ,E ) CY : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-E ,E ) CZ : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-E ,E ) DE : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-E ,E ) DK : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(A ,ABN ) DO : 27 27 27 27 27 27 27 27 27 27 27 27 27 27
(-E ,E ) DZ : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-A ,AB ) EC : 27 27 27 27 27 27 27 27 27 27 27 27 27 27
(-E ,E ) EE : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-E ,E ) EG : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-E ,E ) ES : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-E ,E ) FI : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-E ,E ) FR : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-E ,E ) GB : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-E ,E ) GI : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-E ,E ) GR : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-A NA ) HK : 27 27 27 27 27 27 27 27 27 27 27 27 27 27
(-E ,E ) HR : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-E ,E ) HU : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-E ,ER ) ID : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-E ,E ) IE : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-EI ,IE ) IL : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
```
<table>
<thead>
<tr>
<th>Country Code</th>
<th>Country Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Argentina</td>
</tr>
<tr>
<td>A</td>
<td>Australia</td>
</tr>
<tr>
<td>A</td>
<td>Austria</td>
</tr>
<tr>
<td>A</td>
<td>Bahrain</td>
</tr>
<tr>
<td>A</td>
<td>Bangladesh</td>
</tr>
<tr>
<td>A</td>
<td>Belgium</td>
</tr>
<tr>
<td>A</td>
<td>Brazil</td>
</tr>
<tr>
<td>A</td>
<td>Canada</td>
</tr>
<tr>
<td>A</td>
<td>China</td>
</tr>
<tr>
<td>A</td>
<td>Colombia</td>
</tr>
<tr>
<td>A</td>
<td>Costa Rica</td>
</tr>
<tr>
<td>A</td>
<td>Czech Republic</td>
</tr>
<tr>
<td>A</td>
<td>Denmark</td>
</tr>
<tr>
<td>A</td>
<td>Egypt</td>
</tr>
<tr>
<td>A</td>
<td>Finland</td>
</tr>
<tr>
<td>A</td>
<td>France</td>
</tr>
<tr>
<td>A</td>
<td>Germany</td>
</tr>
<tr>
<td>A</td>
<td>Ghana</td>
</tr>
<tr>
<td>A</td>
<td>Greece</td>
</tr>
<tr>
<td>A</td>
<td>Hong Kong</td>
</tr>
<tr>
<td>A</td>
<td>Hungary</td>
</tr>
<tr>
<td>A</td>
<td>India</td>
</tr>
<tr>
<td>A</td>
<td>Indonesia</td>
</tr>
<tr>
<td>A</td>
<td>Ireland</td>
</tr>
<tr>
<td>A</td>
<td>Italy</td>
</tr>
<tr>
<td>A</td>
<td>Japan</td>
</tr>
<tr>
<td>A</td>
<td>Jordan</td>
</tr>
<tr>
<td>A</td>
<td>Kenya</td>
</tr>
<tr>
<td>A</td>
<td>Korea</td>
</tr>
<tr>
<td>A</td>
<td>Kuwait</td>
</tr>
<tr>
<td>A</td>
<td>Latvia</td>
</tr>
<tr>
<td>A</td>
<td>Lebanon</td>
</tr>
<tr>
<td>A</td>
<td>Lithuania</td>
</tr>
<tr>
<td>A</td>
<td>Luxembourg</td>
</tr>
<tr>
<td>A</td>
<td>Malaysia</td>
</tr>
<tr>
<td>A</td>
<td>Mexico</td>
</tr>
<tr>
<td>A</td>
<td>Mongolia</td>
</tr>
<tr>
<td>A</td>
<td>Morocco</td>
</tr>
<tr>
<td>A</td>
<td>Netherlands</td>
</tr>
<tr>
<td>A</td>
<td>New Zealand</td>
</tr>
<tr>
<td>A</td>
<td>Nicaragua</td>
</tr>
<tr>
<td>A</td>
<td>Nigeria</td>
</tr>
<tr>
<td>A</td>
<td>Panama</td>
</tr>
<tr>
<td>A</td>
<td>Peru</td>
</tr>
<tr>
<td>A</td>
<td>Philippines</td>
</tr>
<tr>
<td>A</td>
<td>Poland</td>
</tr>
<tr>
<td>A</td>
<td>Portugal</td>
</tr>
<tr>
<td>A</td>
<td>Qatar</td>
</tr>
<tr>
<td>A</td>
<td>Romania</td>
</tr>
<tr>
<td>A</td>
<td>Russia</td>
</tr>
<tr>
<td>A</td>
<td>Saudi Arabia</td>
</tr>
<tr>
<td>A</td>
<td>Senegal</td>
</tr>
<tr>
<td>A</td>
<td>Singapore</td>
</tr>
<tr>
<td>A</td>
<td>Slovakia</td>
</tr>
<tr>
<td>A</td>
<td>Slovenia</td>
</tr>
<tr>
<td>A</td>
<td>South Africa</td>
</tr>
<tr>
<td>A</td>
<td>Spain</td>
</tr>
<tr>
<td>A</td>
<td>Sri Lanka</td>
</tr>
<tr>
<td>A</td>
<td>Sweden</td>
</tr>
<tr>
<td>A</td>
<td>Switzerland</td>
</tr>
<tr>
<td>A</td>
<td>Taiwan</td>
</tr>
<tr>
<td>A</td>
<td>Thailand</td>
</tr>
<tr>
<td>A</td>
<td>Turkey</td>
</tr>
<tr>
<td>A</td>
<td>Ukraine</td>
</tr>
<tr>
<td>A</td>
<td>United Arab Emirates</td>
</tr>
<tr>
<td>A</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>A</td>
<td>United States</td>
</tr>
<tr>
<td>A</td>
<td>Venezuela</td>
</tr>
<tr>
<td>A</td>
<td>Viet Nam</td>
</tr>
<tr>
<td>A</td>
<td>Zimbabwe</td>
</tr>
</tbody>
</table>

Note: The table lists country codes and country names as they are used in the Cisco Catalyst 9800 Series Wireless Controller Command Reference.
**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 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**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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.

```plaintext
show wireless exclusionlist [{client mac-address client-mac-addr detail }] [ chassis {chassis-number | active | standby} R0 ]
```

**Syntax Description**
- `client-mac-addr`  SI interferers of type microwave oven for the 2.4-GHz band.
- `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**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to see the wireless exclusion list:

```plaintext
Device# show wireless exclusionlist
```
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

This example shows how to view fabric status:

```
Device# show wireless fabric summary
Fabric Status : Enabled

Control-plane:
Name           Key  Status
-------------------------
test-map 10.12.13.14  test1  Down

Fabric VNID Mapping:
Name L2-VNID L3-VNID       IP Address    Subnet
-------------------------
test1              12   10    10.6.8.9     255.255.255.236
```

Cisco Catalyst 9800 Series Wireless Controller Command Reference, Cisco IOS XE Gibraltar 16.10.x
show wireless fabric client summary

To see the summary of a fabric enabled wireless client, use the `show wireless fabric client summary` command.

Command Default

| Command Default | None |

Command Modes

| 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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

Examples

The following example shows how to see the fabric enabled wireless client summary:

```
Device# show wireless fabric client summary
```
**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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
```

Cisco Catalyst 9800 Series Wireless Controller Command Reference, Cisco IOS XE Gibraltar 16.10.x
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**

- **channel-id**  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>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.3SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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
```
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**

- `channel-id` 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>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.3SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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 media-stream client detail

To see the media stream clients information by stream name, use the `show wireless media-stream client detail` command.

**Command Default**
None

**Command Modes**
Privileged EXEC

**Command History**
-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}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail groupName</td>
<td>Display media-stream group configuration details of the group mentioned in the command.</td>
</tr>
<tr>
<td>summary</td>
<td>Display media-stream group configuration summary</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>User EXEC mode or Privileged EXEC mode</td>
</tr>
</tbody>
</table>

| 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.

```
Device# show wireless media-stream message details
```

<table>
<thead>
<tr>
<th>Command Default</th>
<th>Command Modes</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>Privileged EXEC</td>
</tr>
</tbody>
</table>

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**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.

**Syntax Description**

| ap  | Show joined Access Point in sub-domain. |

**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 Denali 16.3.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>AP name</th>
<th>AP radio MAC</th>
<th>Controller IP</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>bos2kk</td>
<td>00f2.8c42.f520</td>
<td>default-group</td>
<td>default-group</td>
</tr>
<tr>
<td>IosAP1</td>
<td>34ed.522f.7e60</td>
<td>default-group</td>
<td>default-group</td>
</tr>
</tbody>
</table>
```
**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.

```
Device# show wireless media-stream multicast-direct state
```

<table>
<thead>
<tr>
<th>Command Default</th>
<th>Command Modes</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>Privileged EXEC</td>
</tr>
</tbody>
</table>

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>summary</td>
<td>Shows the summary of all connected mesh APs.</td>
</tr>
<tr>
<td>tree</td>
<td>Shows the Mesh AP tree.</td>
</tr>
<tr>
<td>backhaul</td>
<td>Shows the mesh APs backhaul info.</td>
</tr>
<tr>
<td>chassis-number</td>
<td>Enter the chassis number as either 1 or 2.</td>
</tr>
<tr>
<td>active R0</td>
<td>Active instance of the configuration in Route-processor slot 0.</td>
</tr>
<tr>
<td>standby R0</td>
<td>Standby instance of the configuration in Route-processor slot 0.</td>
</tr>
</tbody>
</table>

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**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.
- `chassis-number` 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
</table>
|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.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show wireless mesh ap tree</td>
<td>Shows the mesh AP tree.</td>
</tr>
</tbody>
</table>

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to see the mesh AP tree:

```
Device# 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**

<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>

**Example**

The following example shows how to view the wireless mesh AP tree:

```
Device # show wireless mesh ap tree
```
# 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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>config</td>
<td>Shows the mesh configurations.</td>
</tr>
<tr>
<td>chassis-number</td>
<td>Enter the chassis number as either 1 or 2.</td>
</tr>
<tr>
<td>active R0</td>
<td>Active instance of the active AP filters in Route-processor slot 0.</td>
</tr>
<tr>
<td>standby R0</td>
<td>Standby instance of the active AP filters in Route-processor slot 0.</td>
</tr>
</tbody>
</table>

## 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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

## Examples

The following example shows how to see the mesh configurations:

```
Device# wireless mesh config
```
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**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>neighbor</td>
<td>Shows the neighbors of all connected mesh APs.</td>
</tr>
<tr>
<td>chassis-number</td>
<td>Enter the chassis number as either 1 or 2.</td>
</tr>
<tr>
<td>active R0</td>
<td>Active instance of the active AP filters in Route-processor slot 0.</td>
</tr>
<tr>
<td>standby R0</td>
<td>Standby instance of the active AP filters in Route-processor slot 0.</td>
</tr>
</tbody>
</table>

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to see the neighbors of all connected mesh APs:

```
Device# wireless mesh neighbor
```
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 mobility-agent-ip client summary**: Shows the active clients on a mobility agent.
- **ap-list ip-address ip-address**: 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

This example shows how to display a summary of the mobility manager:

```
Device (config)# show wireless mobility ap-list
```

<table>
<thead>
<tr>
<th>AP name</th>
<th>AP radio MAC</th>
<th>Controller IP</th>
<th>Learnt from</th>
</tr>
</thead>
<tbody>
<tr>
<td>TSIM_AP-101</td>
<td>0000.2000.6600</td>
<td>9.9.9.2</td>
<td>Self</td>
</tr>
<tr>
<td>TSIM_AP-102</td>
<td>0000.2000.6700</td>
<td>9.9.9.2</td>
<td>Self</td>
</tr>
<tr>
<td>TSIM_AP-103</td>
<td>0000.2000.6800</td>
<td>9.9.9.2</td>
<td>Self</td>
</tr>
<tr>
<td>TSIM_AP-400</td>
<td>0000.2001.9100</td>
<td>9.9.9.2</td>
<td>Self</td>
</tr>
<tr>
<td>TSIM_AP-402</td>
<td>0000.2001.9300</td>
<td>9.9.9.2</td>
<td>Self</td>
</tr>
<tr>
<td>TSIM_AP-403</td>
<td>0000.2001.9400</td>
<td>9.9.9.2</td>
<td>Self</td>
</tr>
<tr>
<td>TSIM_AP-406</td>
<td>0000.2001.9700</td>
<td>9.9.9.2</td>
<td>Self</td>
</tr>
<tr>
<td>TSIM_AP-407</td>
<td>0000.2001.9800</td>
<td>9.9.9.2</td>
<td>Self</td>
</tr>
<tr>
<td>TSIM_AP-409</td>
<td>0000.2001.9a00</td>
<td>9.9.9.2</td>
<td>Self</td>
</tr>
</tbody>
</table>
**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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip-address</code></td>
<td>Mobility peer IPv4 IP address.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
</table>
|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
```

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>Privileged EXEC</td>
</tr>
<tr>
<td>Command History</td>
<td>Release</td>
</tr>
<tr>
<td></td>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
</tr>
</tbody>
</table>

**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**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**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 source-ip** *(Optional)* Specifies the source IPv4 and IPv6 address of multicast traffic.
- **group group-ip** *(Optional)* Specifies the destination group and group IP of multicast traffic.
- **vlan vlan-id** Displays the client information on VLAN with the specific VLAN ID.

**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 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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
```
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.
- `group-ip` Specifies the group IP address.
- `vlan vlan-id` Specifies the destination group IPv4/IPv6 Address of multicast traffic.

**Command Default**

None.

**Command Modes**

Privileged EXEC

**Command History**

- **Release**
  - Cisco IOS XE 3.2SE
- **Modification**
  - 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 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**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ap summary</td>
<td>Displays aggressive load balancing configuration of access points configured to the controller.</td>
</tr>
<tr>
<td>client summary</td>
<td>Displays aggressive load balancing configuration details of the clients.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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
```

---

*Cisco Catalyst 9800 Series Wireless Controller Command Reference, Cisco IOS XE Gibraltar 16.10.x*
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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 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**

<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>

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 Name      Weight
Policy Profile  Band   ATF Policy Name      Weight
WGB             2.4GHz - -                  - -
WGB             5GHz - -                    - -
Policy1          2.4GHz - -                  - -
Policy1          5GHz - -                    - -
Test WBG         2.4GHz - -                  - -
Test WBG         5GHz - -                    - -
profile-name     2.4GHz 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.

```plaintext
show wireless profile airtime-fairness summary
```

**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>

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**

- `profile-name`  AP packet capture profile.

**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>

**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
tests1 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
```
<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ARP</td>
<td>Disabled</td>
</tr>
<tr>
<td>IAPP</td>
<td>Disabled</td>
</tr>
<tr>
<td>IP</td>
<td>Disabled</td>
</tr>
<tr>
<td>TCP</td>
<td>Disabled</td>
</tr>
<tr>
<td>TCP port</td>
<td>all</td>
</tr>
<tr>
<td>UDP</td>
<td>Disabled</td>
</tr>
<tr>
<td>UDP port</td>
<td>all</td>
</tr>
<tr>
<td>Broadcast</td>
<td>Disabled</td>
</tr>
<tr>
<td>Multicast</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>3.2SE</td>
<td></td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detailed</td>
<td>Shows the flex-profile detailed parameters</td>
</tr>
<tr>
<td>summary</td>
<td>Show the flex-profile summary.</td>
</tr>
<tr>
<td>chassis-number</td>
<td>Chassis number. Valid range is 1–2.</td>
</tr>
<tr>
<td>active</td>
<td>Active instance.</td>
</tr>
<tr>
<td>standby</td>
<td>Standby instance.</td>
</tr>
<tr>
<td>R0</td>
<td>Route-Processor slot 0.</td>
</tr>
</tbody>
</table>

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**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 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| {mobility|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**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**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.
- **rfid-mac-address**: RFID MAC address.

**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>

**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 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.
- **chassis-number**: 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**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**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**

<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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**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 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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>queue</code></td>
<td>Shows queue statistics of all connected mesh APs.</td>
</tr>
<tr>
<td><code>security</code></td>
<td>Shows security statistics of all connected mesh APs.</td>
</tr>
<tr>
<td><code>chassis-number</code></td>
<td>Enter the chassis number as either 1 or 2.</td>
</tr>
<tr>
<td><code>active R0</code></td>
<td>Active instance of the active AP filters in Route-processor slot 0.</td>
</tr>
<tr>
<td><code>standby R0</code></td>
<td>Standby instance of the active AP filters in Route-processor slot 0.</td>
</tr>
</tbody>
</table>

### 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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to see the security statistics of all connected mesh APs:

```
Device# show wireless stats mesh security
```
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

The following is sample output from the `show wireless summary` command:

```
Device# show wireless summary

Access Point Summary

<table>
<thead>
<tr>
<th>Total</th>
<th>Up</th>
<th>Down</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11a/n</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>802.11b/g/n</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>All APs</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

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 }
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>summary</td>
<td>Displays the summary of all RF tags.</td>
</tr>
<tr>
<td>detailed rf-tag-name</td>
<td>RF tag name.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>Privileged EXEC</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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

<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>

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
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**

<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>

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]
```

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>Privileged EXEC</td>
</tr>
<tr>
<td>Command History</td>
<td><strong>Release</strong></td>
</tr>
<tr>
<td></td>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>mac-address</code></td>
<td>MAC address of the WGB.</td>
</tr>
<tr>
<td><code>detail</code></td>
<td>View clients of the wireless WGB.</td>
</tr>
</tbody>
</table>

**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 in a release earlier than Cisco IOS XE Gibraltar 16.10.1.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>Privileged EXEC</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<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>

**Examples**

The following example shows how to see the active workgroup bridges (WGB):

Device# show wireless wgb summary
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 | detailedmac-addr | friendlysummary | listmac-address mac-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]}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>mac-address</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Modes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privileged EXEC</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Release</strong></td>
</tr>
<tr>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
</tr>
</tbody>
</table>

**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.

**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 3.3SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

`client-mac`  
MAC address of the rogue client.

**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 3.3SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 client summary

To display summary of WPS rogue clients, use the `show wireless wps rogue client summary` command.

**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 3.2SE</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 wps summary

To display Wireless Protection System (WPS) summary information, use the `show wps summary` command.

### Syntax 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
```

### Related Commands

- `config wps signature frequency`
- `config wps signature interval`
- `config wps signature quiet-time`
config wps signature reset
show wps signature events
show wps signature mac-frequency
show wps summary
config wps signature
config wps signature interval
**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.

**Syntax Description**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>shutdown</code></td>
<td>Shuts down the profile and disables network.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

config-rf-profile

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Denali 16.3.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This example shows how to close a RF Profile and disable the network.

```
Device(config-rf-profile)#shutdown
```
shutdown
INDEX

[no] ap remote-lan shutdown command 160

A

aaa accounting update periodic interval-in-minutes 14
aaa authentication login command 16
aaa authorization credential download default command 21
aaa group server ldap command 22
aaa group server radius command 23
aaa local authentication default authorization 24
aaa-override command 31
aaa-policy 32
aaa-realm enable 33
access-list 35
access-list acl-ace-limit 37
accounting-list command 38
acl-policy 39
airtime-fairness mode command 43
allow at-least 5 at-most 10 44
ap auth-list ap-policy 47, 48
ap capwap backup 49
ap capwap multicast 50
ap capwap retransmit 51
ap capwap timers 52
ap edp 54
ap country 55
ap dot11 56
ap dot11 24ghz cleanair command 57, 58
ap dot11 24ghz dot11g 60
ap dot11 24ghz rate 61
ap dot11 24ghz rrm 63
ap dot11 24ghz rrm coverage command 108
ap dot11 24ghz rx-sop threshold 67
ap dot11 5ghz channelswitch mode 68, 77
ap dot11 5ghz channelswitch quiet 69
ap dot11 5ghz cleanair 70
ap dot11 5ghz cleanair command 71
ap dot11 5ghz power-constraint 73
ap dot11 5ghz rate 74
ap dot11 5ghz rrm channel device command 76
ap dot11 5ghz rrm command 102
ap dot11 5ghz rrm tpc-threshold command 116
ap dot11 5ghz rrm txpower command 117, 118
ap dot11 5ghz rx-sop threshold 78
ap dot11 5ghz shutdown 79
ap dot11 5ghz smart-dfs 80
ap dot11 beaconperiod 81
ap dot11 cac media-stream 82
ap dot11 cac video 86
ap dot11 cac voice 88
ap dot11 cleanair 91
ap dot11 cleanair device 92
ap dot11 dot11n 94
ap dot11 dpc 97
ap dot11 dual-band cleanair 128
ap dot11 edcs-parameters 99
ap dot11 multimedia 85
ap dot11 rrm channel cleanair-event 64
ap dot11 rrm channel command 65, 66, 75, 105
ap dot11 rrm channel dca 106
ap dot11 rrm group-member 110
ap dot11 rrm group-mode 111
ap dot11 rrm logging 112
ap dot11 rrm monitor 114
ap dot11 rrm ndp-type 115
ap filter 119
ap fra 120
ap image 122
ap image upgrade 123
ap link-encryption 124
ap name 135, 136, 137, 138, 140, 148
ap name clear-personal-ssid 125
ap name core-dump 126
ap name crash-file 127
ap name dot11 rrm profile 130
ap name mesh block-child 133
ap name mesh daisy-chaining 134
ap name mesh security psk provisioning delete 139
ap name mode 142
ap name mode bridge 144
ap name monitor-mode 145
ap name monitor-mode dot11b 146
ap name priority 147
ap name shutdown 149
ap name sniff 150
ap name tftp-downgrade 151
ap name-regex 154
ap packet-capture start 157
ap profile 158
ap remote-lan profile-name command 159
INDEX

ap remote-lan-policy policy-name command 161
ap tag-source-priority 162
ap tag-sources revalidate 163
assisted-roaming command 166
avg-packet-size packetsize 168

B
bridge-group 176

C
cache timeout active value 179
cache timeout inactive value 180
captive-portal-bypass command 182
chassis clear 189
chassis ha-interface 190
chassis priority 191
chassis timer peer-timeout 192
class command 193
class-map command 197
classify 196
clear ip nbar protocol-discovery wlan 199
clear platform condition all 200
client association limit command 203
client-l2-vnid 206
collect counter command 207
collect wireless ap mac address command 208
commands 476
collection 476
domain-name 476
convergence 210
custom-page login device 221

d debug platform qos-acl-tcam command 224
d debug qos-manager command 225
default command 222
description command 226
destination command 227
device-tracking binding vlan 230
dhcp-tlv-caching command 233
dnscrypt command 235
dot11 5ghz reporting-interval 238
dot11 airtime-fairness command 237

e
eap profile 242
et-analytics command 243
event identity-update 246
exclusionlist command 247

F
fabric control-plane command 248
fallback-radio-shut 249
flex 250

I
idle-timeout 262
inactive-timeout command 264
interface vlan command 265
ip access-group command 266
ip access-list extended 267
ip domain-name 276
ip flow monitor command 277
ip flow-export destination command 278
ip multicast vlan command 287
ip nbar protocol-discovery 268
ip nbar protocol-pack 289
ip verify source command 294
ipv4 dhcp 295
ipv4 flow monitor 296
ipv6 nd managed-config-flag command 307
ipv6 nd ra throttler attach-policy 309
ipv6 traffic-filter command 313

L
ldap attribute-map command 315
ldap server command 316
local-auth ap eap-fast 317
local-site 318
location notify-threshold command 320

M
mac-filtering 322
match (access-map configuration) command 323, 364
match (class-map configuration) command 366
match any 327
match interface command 330
match ipv4 command 331, 332
match ipv4 destination address command 333, 334
match ipv4 source address command 335, 336
match ipv4 ttl command 337, 338
match ipv6 command 339, 340
match ipv6 destination address command 341, 342
match ipv6 hop-limit command 343, 344
match ipv6 source command 345, 346
match non-client-nrt command 348
match protocol command 349
match transport command 354, 355
match transport icmp ipv4 command 356, 357
match transport icmp ipv6 command 358, 359
match user-role 360
match wireless ssid command 362, 363
match wlan user-priority command 370
max-bandwidth 371
media-stream multicast-direct command 515
method fast 374
mobility anchor 375
multicast 379

N
nac command 380
nas-id option2 381
network 362
nmsp cloud-services enable 383
nmsp cloud-services http-proxy 384
nmsp cloud-services server token 385
nmsp cloud-services server url 386
nmsp notification interval command 387

O
office-extend 390
option command 391

P
packet-capture 393
parameter-map type subscriber attribute-to-service 394
parameter-map type umbrella global command 395
peer-blocking command 396
policy command 398
policy 397
policy-map command 401, 403
port 405
priority priority-value 406
priority-queue command 407

Q
qos video 413
queue-limit command 412, 416
queue-set command 418

R
radius server command 419
range 420
reanchor class 421
record wireless avc basic 422
redirect 424
redirect portal 425
remote-lan command 427
remote-span command 426
request platform software trace archive 428
rrc-evaluation 430

S
security 431
security dot1x authentication-list 432
security static-wep-key 438
security web-auth command 439
service-policy command 442, 444
service-policy qos 445
service-template command 446
session-timeout command 447
set command 448
set platform software trace 718, 719
set trace capwap ap ha command 455
set trace mobility ha command 456
set trace qos ap ha command 458
sgl-tag 459
show ap 639
show ap airtime-fairness summary command 574
show ap auth-list 575
show ap config global 578
show ap crash-file 579
show ap dot11 593, 594
show ap dot11 24ghz cleanair device type command 586
show ap dot11 24ghz command 586
show ap dot11 24ghz SI config 589
show ap dot11 24ghz SI device type 590
show ap dot11 5ghz 580, 591
show ap dot11 cleanair summary 596
show ap environment 597
show ap filter all 599
show ap filters active 598
show ap fra 600
show ap gps location 601
show ap hyperlocation cmx summary 606
show ap image 607
show ap link-encryption 608
show ap master list 609
show ap monitor-mode summary 610
show ap name 614, 617, 621, 622, 624, 625, 626, 627, 628, 629
show ap name auto-rf 611
show ap name config 615
show ap name dot11 618
show ap name wlan 630
show ap profile 632
show ap summary 636
show ap tag sources 637
show arp 640
show arp summary 641
show ave client command 642
show ave wlan command 643
show chassis 644
show flow exporter command 653
show flow record command 659
show interfaces command 660
show ip 664
show ip igmp snooping igmpv2-tracking command 667
show wireless vlan details 884
show wireless wgb mac-address 885
show wireless wgb summary 886
show wireless wps rogue 887
show wireless wps rogue ap command 888
show wireless wps rogue client detailed command 889
shutdown command 460
switchport access vlan command 465
switchport command 463
switchport mode command 467
T
tag rf 469
tag site site-tag 470
transport command 471
type command 473
U
udp-timeout command 474
umbrella-param-map command 475
V
violation 478
vlan access-map command 486
vlan command 479
vlan configuration 485
vlan filter command 488
vlan group command 489
W
wgb broadcast-tagging 490
wgb vlan 491
whitelist acl command 492
wireless aaa policy 494, 495
wireless broadcast vlan command 496
wireless client command 497
wireless client mac-address command 500
wireless fabric command 508
wireless fabric control-plane 507
wireless fabric name 509
wireless load-balancing command 510
wireless macro-micro steering transition-threshold 511
wireless media-stream command 512
wireless media-stream message 514
wireless mesh alarm association count 516
wireless mesh alarm high-snr 517
wireless mesh alarm low-snr 518
wireless mesh alarm max-children map 519
wireless mesh alarm max-children rap 520
wireless mesh alarm max-hop 521
wireless mesh alarm parent-change count 522
wireless mesh backhaul bdomain-channels 523
wireless mesh backhaul rrm 524
wireless mesh cac 525
wireless mesh ethernet-bridging allow-bdp 526
wireless mesh security psk provisioning 527
wireless mesh subset-channel-sync 528
wireless mobility 529
wireless mobility group keepalive 531
wireless mobility group mac-address 532
wireless mobility group member ip 533
wireless mobility group multicast-address 534
wireless mobility group name 535
wireless mobility mac-address 537
wireless mobility multicast ipv4 536
wireless multicast 538
wireless profile airtime-fairness command 539
wireless profile fabric 541
wireless profile policy 542
wireless security dot1x command 544
wireless security web-auth retries command 551
wireless tag policy 552
wireless wps ap-authentication command 554
wireless wps client-exclusion command 555
wireless wps rogue command 557
wireless wps rogue detection command 561
wireless wps rogue rule command 562
wireless-default radius server command 564
wlan wlan1 policy policy1 565