# Cisco Catalyst 9800 Series Wireless Controller Command Reference, Cisco IOS XE Gibraltar 16.10.x

**First Published:** 2018-11-20

**Last Modified:** 2019-03-14

**Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

# CONTENTS

PREFACE

CHAPTER 1

CHAPTER 2

# Preface

## Document Conventions

This document uses the following conventions:

| Convention | Description |
|---|---|
| ^ or Ctrl | 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.) |
| **bold** font | Commands and keywords and user-entered text appear in **bold** font. |
| *Italic* font | Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font. |
| `Courier` font | Terminal sessions and information the system displays appear in `courier` font. |
| **`Bold Courier`** font | **`Bold Courier`** font indicates text that the user must enter. |
| [x] | Elements in square brackets are optional. |
| ... | An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated. |
| \| | A vertical line, called a pipe, indicates a choice within a set of keywords or arguments. |
| [x \| y] | Optional alternative keywords are grouped in brackets and separated by vertical bars. |
| {x \| y} | Required alternative keywords are grouped in braces and separated by vertical bars. |

| Convention | Description |
|---|---|
| [x {y \| z}] | Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element. |
| string | A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks. |
| < > | Nonprinting characters such as passwords are in angle brackets. |
| [ ] | Default responses to system prompts are in square brackets. |
| !, # | An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line. |

### 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

Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Read the installation instructions before using, installing, or connecting the system to the power source. Use the statement number at the beginning of each warning statement to locate its translation in the translated safety warnings for this device.

SAVE THESE INSTRUCTIONS

# Related Documentation

**Note** Before installing or upgrading the device, refer to the release notes at https://www.cisco.com/c/en/us/support/wireless/catalyst-9800-series-wireless-controllers/products-release-notes-list.html.

- 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

- Cisco Catalyst 9800-L Wireless Controller documentation, located at:

  http://www.cisco.com/go/c9800

# Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions, and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

## Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

## Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

# Using the Command-Line Interface

# 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*

| Mode | Access Method | Prompt | Exit Method | About This Mode |
|---|---|---|---|---|
| User EXEC | Begin a session using Telnet, SSH, or console. | `Device>` | Enter **logout** or **quit**. | Use this mode to<br>• Change terminal settings.<br>• Perform basic tests.<br>• Display system information. |

| Mode | Access Method | Prompt | Exit Method | About This Mode |
|---|---|---|---|---|
| Privileged EXEC | While in user EXEC mode, enter the **enable** command. | `Device#` | Enter **disable** to exit. | Use this mode to verify commands that you have entered. Use a password to protect access to this mode. |
| Global configuration | While in privileged EXEC mode, enter the **configure** command. | `Device(config)#` | To exit to privileged EXEC mode, enter **exit** or **end**, or press **Ctrl-Z**. | Use this mode to configure parameters that apply to the entire device. |
| VLAN configuration | While in global configuration mode, enter the **vlan** *vlan-id* command. | `Device(config-vlan)#` | To exit to global configuration mode, enter the **exit** command.<br>To return to privileged EXEC mode, press **Ctrl-Z** or enter **end**. | 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. |
| Interface configuration | While in global configuration mode, enter the **interface** command (with a specific interface). | `Device(config-if)#` | To exit to global configuration mode, enter **exit**.<br>To return to privileged EXEC mode, press **Ctrl-Z** or enter **end**. | Use this mode to configure parameters for the Ethernet ports. |
| Line configuration | While in global configuration mode, specify a line with the **line vty** or **line console** command. | `Device(config-line)#` | To exit to global configuration mode, enter **exit**.<br>To return to privileged EXEC mode, press **Ctrl-Z** or enter **end**. | Use this mode to configure parameters for the terminal line. |

# 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 2: Common CLI Error Messages*

| Error Message | Meaning | How to Get Help |
|---|---|---|
| `% Ambiguous command: "show con"` | You did not enter enough characters for your device to recognize the command. | Reenter the command followed by a question mark (?) without any space between the command and the question mark.<br>The possible keywords that you can enter with the command appear. |
| `% Incomplete command.` | You did not enter all of the keywords or values required by this command. | Reenter the command followed by a question mark (?) with a space between the command and the question mark.<br>The possible keywords that you can enter with the command appear. |
| `% Invalid input detected at '^' marker.` | You entered the command incorrectly. The caret (^) marks the point of the error. | Enter a question mark (?) to display all of the commands that are available in this command mode.<br>The possible keywords that you can enter with the command appear. |

# 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

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **help**<br>**Example:**<br>`Device# help` | Obtains a brief description of the help system in any command mode. |
| **Step 2** | *abbreviated-command-entry* **?**<br>**Example:**<br>`Device# di?`<br>`dir disable disconnect` | Obtains a list of commands that begin with a particular character string. |
| **Step 3** | *abbreviated-command-entry* <Tab><br>**Example:**<br>`Device# sh conf<tab>`<br>`Device# show configuration` | Completes a partial command name. |
| **Step 4** | **?**<br>**Example:** | Lists all commands available for a particular command mode. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device>` **`?`** | |
| **Step 5** | *command* **?**<br>**Example:**<br>`Device>` **`show ?`** | Lists the associated keywords for a command. |
| **Step 6** | *command keyword* **?**<br>**Example:**<br>`Device(config)#` **`wireless management ?`**<br>`certificate  Configure certificate details`<br>`interface    Select an interface to configure`<br>`transfer     Active transfer profiles`<br>`trustpoint   Select a trustpoint to configure` | Lists the associated arguments for a keyword. |

# Configuration Commands: a to f

# aaa accounting identity

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

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

## Syntax Description

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

## Command Default

AAA accounting is disabled.

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines

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

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

```
Device# authentication display new-style

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

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

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

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

# aaa accounting update periodic interval-in-minutes

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

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

## Syntax Description

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

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

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

### Examples

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

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

# aaa authentication dot1x

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

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

## Syntax Description

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

## Command Default

No authentication is performed.

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines

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

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

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

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

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

# aaa authentication login

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

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

## Syntax Description

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

## Command Default

None

## Command Modes

Global Configuration

## Command History

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

## Examples

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

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

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

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

# aaa authorization

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

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

## Syntax Description

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

## Command Default

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

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines

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

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

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

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

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

This table describes the method keywords.

*Table 3: aaa authorization Methods*

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

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

Cisco IOS software supports the following methods for authorization:

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

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

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

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

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

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

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

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

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

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

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

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

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

# aaa authorization credential download default

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

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

## Syntax Description

| | |
|---|---|
| *group-name* | Server group name. |

## Command Default

None

## Command Modes

Global Configuration

## Command History

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

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

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

# aaa group server ldap

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

**aaa group server ldap** *group-name*

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

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

This example shows how to configure a AAA server group:

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

# aaa group server radius

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

**aaa group server radius** *group-name*

## Syntax Description

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

## Command Default

None

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines

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

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

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

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

# aaa local authentication default authorization

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

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

## Syntax Description

| | |
|---|---|
| *method-list-name* | Name of the method list. |

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

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

### Examples

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

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

# aaa new-model

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

**aaa new-model**
**no aaa new-model**

## Syntax Description

This command has no arguments or keywords.

## Command Default

AAA is not enabled.

## Command Modes

Global configuration (config)

## Command History

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

## Usage Guidelines

This command enables the AAA access control system.

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

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

The following example shows this restriction:

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

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

## Examples

The following example initializes AAA:

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

## Related Commands

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

# aaa server radius dynamic-author

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

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

## Syntax Description

This command has no arguments or keywords.

## Command Default

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

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines

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

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

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

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

## Examples

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

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

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

## Related Commands

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

# aaa session-id

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

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

## Syntax Description

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

## Command Default

The **common** keyword is enabled.

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines

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

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

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

## Examples

The following example shows how to configure unique session IDs:

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

## Related Commands

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

# aaa-override

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

**aaa-override**

**no aaa-override**

## Syntax Description

This command has no keywords or arguments.

## Command Default

AAA is disabled by default.

## Command Modes

Wireless policy configuration

## Command History

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

This example shows how to enable AAA:

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

# aaa-policy

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

**aaa-policy** *aaa-policy-name*

## Syntax Description

| | |
|---|---|
| *aaa-policy-name* | Name of the AAA policy. |

## Command Default

None

## Command Modes

config-wireless-policy

## Command History

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

### Examples

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

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

# aaa-realm enable

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

**aaa-realm enable**

## Command Default

None

## Command Modes

config-aaa-policy

## Command History

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

### Examples

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

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

# absolute-timer

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

**absolute-timer** *minutes*
**no absolute-timer**

## Syntax Description

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

## Command Default

Disabled (the absolute timeout is 0).

## Command Modes

Service template configuration (config-service-template)

## Command History

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

## Usage Guidelines

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

## Examples

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

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

## Related Commands

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

# access-list

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

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

## Syntax Description

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

## Command Default

None

## Command Modes

Global Config

## Command History

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

### Examples

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

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

# access-list acl-ace-limit

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

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

## Syntax Description

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

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

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

### Examples

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

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

# accounting-list

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

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

## Syntax Description

| | |
|---|---|
| *radius-server-acct* | Accounting RADIUS server name. |

## Command Default

RADIUS server accounting is disabled by default.

## Command Modes

WLAN policy configuration

## Command History

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

## Usage Guidelines

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

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

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

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

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

# acl-policy

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

**acl-policy** *acl-policy-name*

## Syntax Description

| | |
|---|---|
| *acl-policy-name* | Name of the ACL policy. |

## Command Default

None

## Command Modes

config-wireless-flex-profile

## Command History

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

### Examples

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

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

# address

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

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

### Syntax Description

| | |
|---|---|
| *ip-address* | IP address of the remote peer. |

### Command Default

No default behavior or values

### Command Modes

Rsa-pubkey configuration

### Command History

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

### Usage Guidelines

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

### Examples

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

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

### Related Commands

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

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

# address prefix

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

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

## Syntax Description

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

## Command Default

No IPv6 address prefix is assigned.

## Command Modes

DHCP pool configuration (config-dhcpv6)

## Command History

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

## Usage Guidelines

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

## Examples

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

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

## Related Commands

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

# airtime-fairness mode

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

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

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

## Syntax Description

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

## Command Default

None

## Command Modes

RF Profile configuration (config-rf-profile)

## Command History

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

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

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

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

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

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

## Syntax Description

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

## Command Default

None

## Command Modes

config-nd-ra-throttle

## Command History

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

### Examples

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

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

# amsdu (mesh)

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

**amsdu**

## Syntax Description

This command has no keywords or arguments.

## Command Default

amsdu is enabled.

## Command Modes

config-wireless-mesh-profile

## Command History

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

### Example

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

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

# ap

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

**ap** *mac-address*

## Syntax Description

| | |
|---|---|
| *mac-address* | Ethernet MAC address of the AP. |

## Command Default

None

## Command Modes

config

## Command History

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

## Usage Guidelines

none.

### Example

The following example shows how to configure a Cisco AP:

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

# ap auth-list

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

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

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

## Syntax Description

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

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

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

### Example

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

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

# ap auth-list ap-policy

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

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

## Syntax Description

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

## Command Default

None

## Command Modes

Global configuration

## Command History

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

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

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

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

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

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

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

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

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

# ap capwap multicast

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

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

## Syntax Description

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

## Command Default

None

## Command Modes

Global configuration

## Command History

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

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

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

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

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

# ap capwap retransmit

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

**ap profile default-ap-profile**

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

## Syntax Description

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

## Command Default

None

## Command Modes

AP profile configuration (config-ap-profile)

## Command History

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

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

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

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

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

# ap capwap timers

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

**ap profile default-ap-profile**

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

## Syntax Description

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

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

## Command Default

None

## Command Modes

AP profile mode (config-ap-profile)

## Command History

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

# ap country

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

**ap country** *country-code*

## Syntax Description

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

## Command Default

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

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines

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

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

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

# ap dot11 24ghz cleanair

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

**ap dot11 24ghz cleanair**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Disabled.

## Command Modes

Global configuration (config).

## Command History

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

## Usage Guidelines

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

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

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

# default ap dot11 24ghz cleanair device

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

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

## Syntax Description

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

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

## Command Default

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

## Command Modes

Global configuration (config).

## Command History

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

## Usage Guidelines

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

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

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

# ap dot11 24ghz dot11g

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

**ap dot11 24ghz dot11g**
**no ap dot11 24ghz dot11g**

## Syntax Description

This command has no keywords and arguments.

## Command Default

Enabled

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines

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

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

This example shows how to enable the 802.11g network:

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

# ap dot11 24ghz rate

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

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

## Syntax Description

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

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

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

### Examples

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

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

# ap dot11 24ghz rrm channel cleanair-event

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

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

## Syntax Description

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

## Command Default

EDRRM is disabled and the sensitivity is low.

## Command Modes

Global configuration (config).

## Command History

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

## Usage Guidelines

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

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

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

# ap dot11 24ghz rrm channel device

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

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

## Syntax Description

This command has no arguments or keywords.

## Command Default

Persistent device avoidance is disabled.

## Command Modes

Global configuration (config).

## Command History

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

## Usage Guidelines

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

This example shows how to enable persistent device avoidance:

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

# ap dot11 24ghz rrm optimized-roam

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

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

## Syntax Description

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

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

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

### Examples

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

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

# ap dot11 24ghz rx-sop threshold

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

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

## Syntax Description

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

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

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

## Usage Guidelines

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

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

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

### Examples

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

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

# ap dot11 24ghz shutdown

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

**ap dot11 24ghz shutdown**

### Command Default

None

### Command Modes

Global configuration (config)

### Command History

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

### Examples

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

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

# ap dot11 5ghz channelswitch quiet

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

**ap dot11 5ghz channelswitch quiet**

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

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

### Examples

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

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

# ap dot11 5ghz cleanair

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

**ap dot11 5ghz cleanair**

## Command Default

Disabled.

## Command Modes

Global configuration.

## Command History

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

## Usage Guidelines

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

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

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

# default ap dot11 5ghz cleanair device

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

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

## Syntax Description

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

## Command Default

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

## Command Modes

Global configuration (config).

## Command History

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

## Usage Guidelines

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

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

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

# ap dot11 5ghz power-constraint

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

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

## Syntax Description

| | |
|---|---|
| *value* | 802.11h power constraint value.<br>**Note** The range is from 0 to 30 dBm. |

## Command Default

None

## Command Modes

Global configuration

## Command History

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

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

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

# ap dot11 5ghz rate

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

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

## Syntax Description

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

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

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

### Examples

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

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

# ap dot11 5ghz rrm channel cleanair-event

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

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

## Syntax Description

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

## Command Default

EDRRM is disabled and the EDRRM sensitivity is low.

## Command Modes

Global configuration (config).

## Command History

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

## Usage Guidelines

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

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

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

# ap dot11 5ghz rrm channel device

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

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

## Syntax Description

This command has no arguments or keywords.

## Command Default

The CleanAir persistent device state is disabled.

## Command Modes

Global configuration (config)

## Command History

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

## Usage Guidelines

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

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

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

# ap dot11 5ghz rx-sop threshold

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

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

## Syntax Description

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

## Command Default

None

## Command Modes

config

## Command History

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

## Usage Guidelines

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

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

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

### Examples

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

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

# ap dot11 5ghz shutdown

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

**ap dot11 5ghz shutdown**

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

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

### Examples

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

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

# ap dot11 5ghz smart-dfs

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

**ap dot11 5ghz smart-dfs**

## Command Default

None

## Command Modes

config

## Command History

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

### Examples

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

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

# ap dot11

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

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

## Syntax Description

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

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

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

### Examples

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

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

# ap dot11 beaconperiod

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

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

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

## Syntax Description

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

## Command Default

None

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines

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

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

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

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

# ap dot11 cac media-stream

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

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

## Syntax Description

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

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

## Command Default

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

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines

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

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

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

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

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

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

# ap dot11 cac multimedia

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

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

## Syntax Description

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

## Command Default

The default value is 75%.

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines

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

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

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

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

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

# ap dot11 cac voice

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

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

## Syntax Description

| | |
|---|---|
| **24ghz** | Specifies the 2.4 GHz band. |
| **5ghz** | Specifies the 5 GHz band. |
| **acm** | Enables bandwidth-based voice CAC for the 2.4 GHz or 5 GHz band.<br>**Note** To disable bandwidth-based voice CAC for the 2.4 GHz or 5 GHz band, use the **no ap dot11** {**24ghz \| 5ghz**} **cac voice acm** command. |
| **load-based** | Enable load-based CAC on voice access category.<br>**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:<br>• 64kbps—Specifies CAC parameters for the SIP G711 codec.<br>• 8kbps—Specifies CAC parameters for the SIP G729 codec.<br>**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.<br>**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.<br>**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.<br>**Note** The default is **ignore** (disabled). |

### Command Default

None

### Command Modes

Global configuration

## Command History

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

## Usage Guidelines

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

# ap dot11 cleanair

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

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

## Syntax Description

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

## Command Default

Disabled

## Command Modes

Global configuration

## Command History

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

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

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

# ap dot11 cleanair device

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

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

## Syntax Description

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

## Command Default

None

## Command Modes

Global configuration

**Command History**

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

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

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

# ap dot11 dot11n

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

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

## Syntax Description

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

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

### Command Default

By default, priority 0 is enabled.

### Command Modes

Global configuration

### Command History

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

### Usage Guidelines

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

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

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

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

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

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

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

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

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

This example shows how to enable only long guard intervals:

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

This example shows how to specify MCS rates:

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

This example shows how to enable RIFS:

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

# ap dot11 dtpc

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

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

## Syntax Description

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

## Command Default

None

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines

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

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

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

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

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

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

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

# ap dot11 edca-parameters

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

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

## Syntax Description

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

## Command Default

**wmm-default**

## Command Modes

Global configuration

## Command History

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

This example shows how to enable SpectraLink voice priority parameters:

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

# ap dot11 load-balancing denial

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

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

### Syntax Description

| | |
|---|---|
| *count* | Load balancing denial count. |

### Command Default

None

### Command Modes

Global configuration (config)

### Command History

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

#### Example

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

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

# ap dot11 load-balancing window

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

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

## Syntax Description

| | |
|---|---|
| *clients* | Number of clients. Valid range is from 0 to 20. |

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

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

### Example

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

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

# ap dot11 rf-profile

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

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

## Syntax Description

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

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

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

## Usage Guidelines

None

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

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

# ap dot11 rrm

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

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

## Syntax Description

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

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

## Command Default

Disabled

## Command Modes

Interface configuration

## Command History

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

## Usage Guidelines

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

This example shows how to configure various RRM settings.

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

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

# ap dot11 rrm channel

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

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

## Syntax Description

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

## Command Default

None.

## Command Modes

Interface configuration.

## Command History

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

## Usage Guidelines

None.

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

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

# ap dot11 rrm channel cleanair-event

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

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

## Syntax Description

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

## Command Default

None

## Command Modes

Global configuration

## Command History

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

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

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

# ap dot11 rrm channel dca

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

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

## Syntax Description

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

## Command Default

None

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines

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

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

*Table 6: DCA Sensitivity Threshold*

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

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

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

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

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

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

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

# ap dot11 rrm coverage

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

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

## Syntax Description

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

## Command Default

None.

## Command Modes

Interface configuration.

## Command History

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

## Usage Guidelines

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

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

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

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

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

# ap dot11 rrm group-member

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

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

## Syntax Description

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

## Command Default

None

## Command Modes

Global configuration

## Command History

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

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

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

# ap dot11 rrm group-mode

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

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

## Syntax Description

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

## Command Default

auto

## Command Modes

Global configuration

## Command History

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

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

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

# ap dot11 rrm logging

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

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

## Syntax Description

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

## Command Default

Disabled

## Command Modes

Global configuration

## Command History

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

# ap dot11 rrm monitor

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

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

## Syntax Description

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

## Command Default

None

## Command Modes

Global configuration

## Command History

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

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

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

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

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

# ap dot11 rrm ndp-type

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

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

## Syntax Description

| | |
|---|---|
| **24ghz** | Specifies the 2.4-GHz band. |
| **5ghz** | Specifies the 5-GHz band. |
| **6ghz** | Specifies the 6-GHz band. |
| **protected** | Specifies the Tx RRM protected (encrypted) neighbor discovery protocol. |
| **transparent** | Specifies the Tx RRM transparent (not encrypted) neighbor discovery protocol. |

## Command Default

None

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |
| Cisco IOS XE Cupertino 17.7.1 | This command was modified with the introduction of the 6-GHz band. |

## Usage Guidelines

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

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

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

# ap dot11 rrm tpc-threshold

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

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

## Syntax Description

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

## Command Default

None.

## Command Modes

Interface configuration.

## Command History

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

## Usage Guidelines

None.

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

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

# ap dot11 rrm txpower

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

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

## Syntax Description

| | |
|---|---|
| **auto** | Enables auto-RF. |
| **max** *powerLevel* | Configures maximum auto-RF tx power. The range is between -10 to -30. |
| **min** *powerLevel* | Configures minimum auto-RF tx power. The range is between -10 to -30. |
| **once** | Enables one-time auto-RF. |

## Command Default

None.

## Command Modes

Interface configuration.

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |
| | The **no** form of the command is introduced. |

## Usage Guidelines

None.

This example shows how to enables auto-RF once.

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

# ap dot11 rrm txpower

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

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

## Syntax Description

| | |
|---|---|
| **auto** | Enables auto-RF. |
| **max** *powerLevel* | Configures maximum auto-RF tx power. The range is between -10 to -30. |
| **min** *powerLevel* | Configures minimum auto-RF tx power. The range is between -10 to -30. |
| **once** | Enables one-time auto-RF. |

## Command Default

None.

## Command Modes

Interface configuration.

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |
| | The **no** form of the command is introduced. |

## Usage Guidelines

None.

This example shows how to enables auto-RF once.

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

# ap filter

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

**ap filter** { { **name** *filter-name* } **type** { **tag** } | { **priority** *priority-number* | **filter-name** *filter-name* } }

## Syntax Description

| Parameter | Description |
|---|---|
| **priority** | Set the priority for a named filter. |
| *priority-number* | The valid AP filter priority range is 0 to 1023. |
| *filter-name* | Enter the name for the ap filter. |
| **type** | Type of filter. |
| **tag** | Filter to assign AP Tags. Tag filter may be persistent based on tag persistence on the global configuration. |

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

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

### Examples

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

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap filter name test-filter
Device(config)# ap filter name test-filter type priming
Device(config)# ap filter priority 12 filter-name test-filter
```

# ap fra

To configure flexible radio assignment (FRA) and its parameters, use the **ap fra** command.

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

## Syntax Description

| | |
|---|---|
| **interval** *no-of-hours* | Enter the number of hours for the FRA interval. Valid range is 1 to 24 hours. |
| **sensitivity** {**high** \| **low** \| **medium**} | Configures the FRA coverage overlap sensitivity as high, low, or medium. |
| **sensor-threshold** {**balanced** \| **client-preferred** \| **client-priority** \| **sensor-preferred** \| **sensor-priority**} | Configures FRA sensor threshold to one of the available options. |
| **service-priority** {**coverage** \| **service-assurance**} | Configures FRA service priority to Coverage or Service Assurance. |

## Command Default

None

## Command Modes

config

## Command History

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

## Usage Guidelines

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

### Examples

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

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap fra interval 8
```

# ap fra 5-6ghz interval

To configure the Flexible Radio Assignment (FRA) 5/6-GHz interval in hours, use the **ap fra 5-6ghz interval** command.

**ap fra 5-6ghz interval** *number-of-hours*

## Syntax Description

| | |
|---|---|
| *number-of-hours* | Specifies the FRA 5/6-GHz interval in hours. The value range is between 1 to 24 hours. |

## Command Default

None

## Command Modes

Global Configuration

## Command History

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

### Example

This example shows how to configure the Flexible Radio Assignment (FRA) 5/6-GHz interval in hours:

```
Device(config)# ap fra 5-6ghz interval 12
```

# ap hyperlocation

To configure hyperlocation and related parameters, use the **ap hyperlocation** command. To disable hyperlocation and related parameters, use the **no** form of this command.

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

## Syntax Description

| | |
|---|---|
| **ble-beacon** | Enables BLE beacon parameters. |
| *beacon-id* | BLE beacon ID. The range is from 1 to 4. |
| **interval** | Sets the BLE beacon interval. |
| *interval-value* | BLE beacon interval value, in hertz. The range is from 1 to 10. The default is1. |
| **threshold detection** *value-in-dBm* | Sets threshold to filter out packets with low RSSI. The **[no]** form of the command resets the threshold to its default value. |
| **threshold reset** *value-btwn-0-99* | Resets value in scan cycles after trigger. The **[no]** form of the command resets the threshold to its default value. |
| **threshold trigger** *value-btwn-1-100* | Sets the number of scan cycles before sending a BAR to clients. The **[no]** form of the command resets the threshold to its default value.<br>**Note** Ensure that the hyperlocation threshold reset value is less than the threshold trigger value. |

## Command History

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

# ap image

To configure an image on all access points that are associated to the device, use the **ap image** command.

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

## Syntax Description

| | |
|---|---|
| **predownload** | Instructs all the access points to start predownloading an image. |
| **reset** | Instructs all the access points to reboot. |
| **swap** | Instructs all the access points to swap the image. |

## Command Default

None

## Command Modes

Any command mode

## Command History

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

This example shows how to 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**]

## Syntax Description

| | |
|---|---|
| **abort** | Cancels AP image upgrade. |
| **destination** *controller-name* {*controller-ipv4-addr* \| *controller-ipv6-addr*} | Instructs all the APs to associate with the destination controller whose name and IP address you must enter. |
| **dry-run** | Runs the rolling AP image upgrade in dry-run mode. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

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

### Examples

The following example shows how to cancel an AP image upgrade:

```
Device# ap image upgrade abort
```

# ap link-encryption

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

**ap link-encryption**
**no ap link-encryption**

### Syntax Description

This command has no keywords and arguments.

### Command Default

Disabled

### Command Modes

Global configuration

### Command History

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

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

```
Device(config)# ap link-encryption
```

# ap name antenna band mode

To configure the antenna mode, use the **ap name***ap- name* **antenna-band-mode{ single | dual }** command.

**ap name***ap-name* **antenna-band-mode** {**single** | **dual**}

## Syntax Description

| | |
|---|---|
| *ap- name* | Name of the Cisco lightweight access point. |
| **antenna-band-mode** | Instructs the access point to enable the band mode of antenna. |

## Command Default

None

## Command Modes

Privileged EXEC(#)

## Command History

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

### Example

This example shows how to configure the antenna band mode of access point.

```
Deviceap name <ap-name> antenna-band-mode single
```

# ap name ble

To enable the able ltx state on the AP, use the **ap name** *ap name* **ble** command.

**ap name** *ap_name* **antena-band-mode {admin | ibeacon | interval | no-advertisement | sync | vibeacon}**

## Syntax Description

| | |
|---|---|
| **ap name** | AP Name |
| **admin** | Enables the ble ltx admin state. |
| **ibeacon** | Enables the BLE LTX iBeacon configuration. |
| **interval** | Enables the BLE LTX scan configuration interval. |
| **no-advertisement** | Enables the BLE LTX No Advertisement. |
| **Sync** | Enables the BLE LTX synchronize. |
| **vibeacon** | Enables the BLE LTX viBeacon configuration. |

## Command Default

Disabled

## Command Modes

Privileged EXEC (#)

## Command History

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

## Examples

The following example shows how to enable ble on the AP:

```
Device# ap name test ble
```

# ap name clear-personal-ssid

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

**ap name** *ap-name* **clear-personal-ssid**

## Syntax Description

| | |
|---|---|
| *ap-name* | AP name. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

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

### Examples

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

```
Device# ap name my-oeap clear-personal-ssid
```

# ap name controller

To configure the controller on the AP, use the **ap name** *ap name* **controller** command.

**ap name** *ap_name* **controller {primary | secondary | tertiary}** *name {A.B.C.D | X:X:X::XX}*

## Syntax Description

| | |
|---|---|
| **ap name** | AP Name |
| **controller** | Configures the controller. |
| **primary** | Configures the primary controller. |
| **secondary** | Configures the secondary controller. |
| **tertiary** | Configures the tertiary controller. |
| *name* | Specifies the name of the primary controller, secondary controller, or tertiary controller. |
| *A.B.C.D* | Specifies theIPv4 address of the primary controller, secondary controller, or tertiary controller. |
| *X:X:X::XX* | Specifies theIPv6 address of the primary controller, secondary controller, or tertiary controller. |

## Command Default

Disabled

## Command Modes

Privileged EXEC (#)

## Command History

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

## Examples

The following example shows how to configure the controller on the AP:

```
Device# ap name cisco-ap controller primary cisco-primary-controller 10.1.1.1
```

# ap name core-dump

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

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

## Syntax Description

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

## Command Default

None

## Command Modes

Privileged EXEC(#)

## Command History

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

## Usage Guidelines

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

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

```
Device# ap name AP2 core-dump 192.1.1.1 log compress
```

# ap name country

To configure the country of operation for a Cisco lightweight access point, use the **ap name country** command.

**ap name** *ap-name* **country** *country-code*

## Syntax Description

| | |
|---|---|
| *ap-name* | Name of the Cisco lightweight access point. |
| *country-code* | Two-letter or three-letter country code. |

## Command Default

None

## Command Modes

Privileged EXEC(#)

## Command History

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

## Usage Guidelines

Cisco devices must be installed by a network administrator or qualified IT professional and the installer must select the proper country code. Following installation, access to the unit should be password protected by the installer to maintain compliance with regulatory requirements and to ensure proper unit functionality. See the related product guide for the most recent country codes and regulatory domains. Also, access point regulatory domains are defined during the access point manufacturing process. You can change the access point country code if the new country code matches a country that is valid within the access point regulatory domain. If you try to enter a country that is not valid to the access point regulatory domain, the command fails.

This example shows how to configure the Cisco lightweight access point's country code to DE:

```
Device# ap name AP2 country JP
```

# ap name crash-file

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

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

## Syntax Description

| | |
|---|---|
| *ap-name* | Name of the Cisco lightweight access point. |
| **get-crash-data** | Collects the latest crash data for a Cisco lightweight access point. |
| **get-radio-core-dump** | Gets a Cisco lightweight access point's radio core dump |
| **slot** | Slot ID for Cisco access point. |
| **0** | Specifies Slot 0. |
| **1** | Specifies Slot 1. |

## Command Default

None

## Command Modes

Privileged EXEC(#)

## Command History

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

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

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

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

```
Device# ap name AP02 crash-file get-radio-core-dump slot 0
```

# ap name dot11 24ghz slot 0 SI

To enable Spectrum Intelligence (SI) for the dedicated 2.4-GHz radio hosted on slot 0 for a specific access point, use the **ap name dot11 24ghz slot 0 SI** command.

**ap name** *ap-name***dot11** { **24ghz** | **5ghz** | **dual-band** | **rx-dual-band** } **slot***slot ID***SI**

## Syntax Description

| | |
|---|---|
| *ap_name* | Name of the Cisco Access Point. |
| **slot 0** | Enables Spectrum Intelligence (SI) for the dedicated 2.4-GHz radio hosted on slot 0 for a specific access point.<br>Here, 0 refers to the Slot ID. |

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

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

### Example

The following example shows how to configure Spectrum Intelligence of an AP.

```
Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 SI
```

# ap name dot11 24ghz slot antenna

To configure the 802.11b antenna hosted on slot 0, use the **ap name dot11 24ghz slot antenna** command.

**ap name** *ap-name***dot1124ghzslot 0antenna**{**ext-ant-gain** *antenna-gain-value* | **selection** [**internal** | **external**}

## Syntax Description

| | |
|---|---|
| *ap-name* | Name of the AP. |
| **24ghz** | Configures 802.11b parameters. |
| **slot** | Sets the slot ID for the Cisco Access Point. |
| **antenna** | Configures the 802.11b Antenna. |
| **ext-ant-gain** | Configures the 802.11b External Antenna Gain. The value range is 0 - 4294967295.<br>Enter External Antenna Gain value in multiple of .5 dBi units (i.e. An integer value 4 means 4 x 0.5 = 2 dBi of gain) |
| **selection** | Configure the 802.11b Antenna selection (internal/external) |

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

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

## Usage Guidelines

### Example

The following example shows how to configure the channel width of an AP.

```
Device# ap name ax1 dot11 24ghz slot 0 antenna selection external
```

# ap name dot11 24ghz slot beamforming

To configures beamforming for the 2.4-GHz radio hosted on slot 0 for a specific access point, use the **ap name dot11 24ghz slot beamforming** command.

**ap name** *ap-name***dot1124ghzslot 0beamforming**

## Syntax Description

| | |
|---|---|
| **beamforming** | Enable 802.11b tx beamforming - 5 GHz |

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

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

## Usage Guidelines

### Example

The following example shows how to configure beamforming of an AP.

```
Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 beamforming
```

# ap name dot11 24ghz slot channel

To configure advanced 802.11 channel assignment parameters for Cisco AP, use the **ap name dot11 24ghz slot channel** command.

**ap name** *ap-name* **dot11 24ghz slot 0 channel** { *channel_number* | **auto** }

## Syntax Description

| | |
|---|---|
| *channel_number* | Advanced 802.11 channel assignment parameters for Cisco AP. Enter a channel number from 1 - 14. |
| **auto** | Enables auto RF. |

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

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

## Usage Guidelines

### Example

The following example shows how to configure the channel of an AP.

```
Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 channel auto
```

# ap name dot11 24ghz slot cleanair

To enable CleanAir for 802.11b radio hosted on slot 0 for a specific access point, use the **ap name dot11 24ghz slot cleanair** command.

**ap name** *ap-name* **dot11 24ghz slot 0 cleanair**

### Syntax Description

| | |
|---|---|
| **cleanair** | Enables 802.11b cleanair management |

### Command Default

None

### Command Modes

Privileged EXEC (#)

### Command History

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

### Example

The following example shows how to configure the cleanair of an AP.

```
Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 cleanair
```

# ap name dot11 24ghz slot dot11n antenna

To configure 802.11n antenna for 2.4-GHz radio hosted on slot 0 for a specific access point, use the **ap name dot11 24ghz slot dot11n antenna** command.

**ap name** *ap-name* **dot11 24ghz slot 0 dot11n antenna** { **A** | **B** | **C** | **D** }

## Syntax Description

| | |
|---|---|
| **dot11n** | Configures 802.11n antenna for 2.4-GHz radio hosted on slot 0 for a specific access point. |
| **antenna** | Configures the 802.11n - 2.4 GHz antenna selection from antenna ports A, B, C, and D. |

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

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

### Example

The following example shows how to configure the channel width of an AP.

```
Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 dot11n antenna A
```

# ap name dot11 24ghz slot dot11ax bss-color

To set the BSS color on the 2.4 GHz, 5 GHz, or dual-band radio, for a specific access point, use the **ap name dot11 24ghz slot dot11ax bss-color** command.

**ap name** *ap-name* **dot11 24ghz slot 0 dot11ax bss-color** *<1-63>*

## Syntax Description

| | |
|---|---|
| **bss-color** | Configures 802.11ax-2.4GHz BSS color |

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

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

### Example

The following example shows how to disable 802.11b radio on Cisco AP.

```
Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 dot11ax bss-color 3
```

# ap name dot11 24ghz slot shutdown

To disable 802.11b radio hosted on slot 0 for a specific access point, use the **ap name dot11 24ghz slot shutdown** command.

**ap name** *ap-name* **dot11 24ghz slot 0 shutdown**

## Syntax Description

| | |
|---|---|
| **shutdown** | Disables 802.11b radio on Cisco AP |

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

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

### Example

The following example shows how to disable 802.11b radio on Cisco AP.

```
Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 shutdown
```

# ap name dot11 dual-band cleanair

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

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

## Syntax Description

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

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

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

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

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

# ap name dot11 dual-band shutdown

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

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

## Syntax Description

| | |
|---|---|
| *ap-name* | Name of the Cisco AP. |
| **shutdown** | Disables the dual band radio on the Cisco AP. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

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

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

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

# ap name dot11 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.<br>**Note** The default client threshold is 12. |
| **customize** | Turns on performance profile customization for an access point.<br>**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.<br>**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.<br>**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.<br>**Note** The default is 1,000,000 bytes per second. |
| **utilization** | Sets the RF utilization threshold.<br>**Note** The operating system generates a trap when this threshold is exceeded. |
| *value* | 802.11 RF utilization threshold from 0 to 100 percent.<br>**Note** The default is 80 percent. |

### Command Default

None

### Command Modes

Privileged EXEC(#)

### Command History

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

This example shows how to set the AP1 clients threshold to 75 clients:

```
Device# ap name AP1 dot11 24ghz rrm profile clients 75
```

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

```
Device# ap name AP1 dot11 5ghz rrm profile customize
```

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

```
Device# ap name AP1 dot11 5ghz rrm profile foreign 0
```

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

```
Device# ap name AP1 dot11 5ghz rrm profile noise 0
```

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

```
Device# ap name AP1 dot11 5ghz rrm profile throughput 10000000
```

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

```
Device# ap name AP1 dot11 5ghz rrm profile utilization 100
```

# ap name hyperlocation

To configure hyperlocation and related parameters for an access point (AP), use the **ap name hyperlocation** command. To disable hyperlocation and related parameters, use the **no** form of this command.

**ap name** *ap-name* **hyperlocation ble-beacon** *beacon-id* { **major** *major-value* | **minor** *minor-value* | **txpwr** *att-value* }

## Syntax Description

| | |
|---|---|
| *ap-name* | Access point name. |
| **ble-beacon** | Configures BLE beacon parameters. |
| *beacon-id* | BLE beacon ID. |
| **major** | Configures BLE beacon major parameter. |
| *major-value* | BLE beacon major value. The range is from 0 to 65535. The default is 0. |
| **minor** | Configures BLE beacon minor parameter. |
| *minor-value* | BLE beacon minor value. The range is from 0 to 65535. The default is 0. |
| **txpwr** | Configures BLE beacon attenuation level. |
| *att-value* | BLE beacon attenuation value, in dBm. The range is from 0 to 52. The default is 0. |

## Command Default

BLE beacon details are not configured.

## Command Modes

Privileged EXEC (#)

## Command History

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

### Example

This example shows how to configure hyperlocation and related parameters for an AP:

```
Device# ap name test-ap hyperlocation ble-beacon 3 txpwr 50
```

# ap name image

To configure an image on a specific access point, use the **ap name image** command.

**ap name** *ap-name* **image** {**predownload** | **swap**}

## Syntax Description

| | |
|---|---|
| *ap-name* | Name of the Cisco lightweight access point. |
| **predownload** | Instructs the access point to start the image predownload. |
| **swap** | Instructs the access point to swap the image. |

## Command Default

None

## Command Modes

Privileged EXEC(#)

## Command History

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

This example shows how to predownload an image to an access point:

```
Device# ap name AP2 image predownload
```

This example shows how to swap an access point's primary and secondary images:

```
Device# ap name AP2 image swap
```

# ap name indoor

To enable the access point in the indoor mode, use the **ap name** *ap name* **indoor** command.

**ap name** *ap_name* **indoor**

## Syntax Description

| | |
|---|---|
| **ap name** | AP Name |
| **indoor** | Enables the access point in the indoor mode. |

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

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

## Examples

The following example shows how to enable the access point in the indoor mode:

```
Device# ap name test indoor
```

# ap name ipsla

To configure ipsla on the AP, use the **ap name** *ap name* **ipsla** command.

**ap name** *ap_name* **ipsla**

## Syntax Description

| | |
|---|---|
| **ap name** | AP Name |
| **ipsla** | Enables the ipsla on the access point. |

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

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

## Examples

The following example shows how to configure ipsla on the access point:

```
Device# ap name test ipsla
```

# ap name keepalive

To enable the keepalive option on the AP, use the **ap name** *ap name* **keepalive** command.

**ap name** *ap_name* **keepalive**

## Syntax Description

This command has no arguments or keywords.

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 17.03.1 | This command was introduced. |

## Examples

The following example shows how to enable the keepalive option on the AP:

```
Device# ap name test keepalive
```

# ap name lan

To configure LAN port configurations for APs, use the **ap name lan** command. To remove LAN port configurations for APs, use the**ap name no lan** command.

**ap name** *ap-name* **[ no ]lan** **port-id** *port-id* {**shutdown** | **vlan-access**}

## Syntax Description

| | |
|---|---|
| **no** | Removes LAN port configurations. |
| **port-id** | Configures the port. |
| *port-id* | The ID of the port. The range is 1-4 |
| **shotdown** | Disables the Port. |
| **vlan-access** | Enables VLAN access to Port. |

## Command Default

None

## Command Modes

Privileged EXEC(#)

## Command History

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

This example shows how to enable VLAN access to port:

```
Device# ap name AP1 lan port-id 1 vlan-access
```

# ap name led

To enable the LED state for an access point, use the **ap name led** command. To disable the LED state for an access point, use the **no** form of this command.

**ap name** *ap-name* **led**
**no ap name** *ap-name* [**led**] **led**

## Syntax Description

| | |
|---|---|
| *ap-name* | Name of the Cisco lightweight access point. |
| **led** | Enables the access point’s LED state. |

## Command Default

None

## Command Modes

Privileged EXEC(#)

## Command History

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

This example shows how to enable the LED state for an access point:

```
Device# ap name AP2 led
```

This example shows how to disable the LED state for an access point:

```
Device# ap name AP2 no led
```

# ap name led-brightness-level

To configure the LED brightness level on the AP, use the **ap name** *ap name* **led-brightness-level** command.

**ap name** *ap_name* **led-brightness-level {1–8}**

## Syntax Description

| | |
|---|---|
| **ap name** | AP Name |
| **led brightness level** | Configures the led brightness level.<br>**Note** Valid led brightness level is from 1 to 8. |

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

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

## Examples

The following example shows the LED brightness level on the access point:

```
Device# ap name cisco-ap led-brightness-level2
```

# ap name location

To modify the descriptive location of a Cisco lightweight access point, use the **ap name location** command.

**ap name** *ap-name* **location** *location*

## Syntax Description

| | |
|---|---|
| *ap-name* | Name of the Cisco lightweight access point. |
| *location* | Location name of the access point (enclosed by double quotation marks). |

## Command Default

None

## Command Modes

Privileged EXEC(#)

## Command History

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

## Usage Guidelines

The Cisco lightweight access point must be disabled before changing this parameter.

This example shows how to configure the descriptive location for access point AP1:

```
Device# ap name AP1 location Building1
```

# ap name mdsn-ap

To configure mdsn-ap on the AP, use the **ap name** *ap name* **mdsn-ap** command.

**ap name** *ap_name* **mdsn-ap {disable | enable | vlan}** *add delete*

## Syntax Description

| | |
|---|---|
| **ap name** | AP Name |
| **disable** | Disables the mDNS access point. |
| **enable** | Enables the mDNS access point. |
| **vlan** | Adds or deletes the VLAN from mDNS access point. |
| *add* | Adds vlan to mDNS AP. |
| *add* | Deletes vlan from the mDNS AP. |

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

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

## Examples

The following example shows how to enable mdns on the AP:

```
Device# Device# ap name test mdns enable
```

# ap name name new-ap-name

To configure the new Cisco AP name, use the **ap name** *ap name* **name** *new-ap-name* command.

**ap name** *ap_name* **name** *new-ap-name*

### Syntax Description

| | |
|---|---|
| **ap name** | AP Name |
| **name** | Specifies the new Cisco AP name. |

### Command Default

None

### Command Modes

Privileged EXEC (#)

### Command History

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

### Examples

The following example shows how to configure the new Cisco AP:

```
Device# ap name test name test2
```

# ap name no

To negate a command or set its defaults on the AP, use the **no** command.

**ap name** *ap_name* **no**

## Syntax Description

| | |
|---|---|
| **ap name** | AP Name |
| **no** | Negate a command or set its defaults. |

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

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

## Examples

The following example shows how to negate a command or set its defaults on the AP:

```
Device# ap name test no
```

# ap name mesh block-child

To set mesh block-child state for a mesh AP, use the **ap name mesh block-child** command.

**ap name** *ap-name* **mesh block-child**

## Syntax Description

| | |
|---|---|
| *ap-name* | Name of the mesh AP. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

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

### Examples

The following example shows how to configure the mesh block-child state for a mesh AP:

```
Device# ap name mymeshap mesh block-child
```

# ap name mesh daisy-chaining

To configure daisy-chain mode for a mesh AP, use the **ap name** *ap-name* **mesh daisy-chaining** command.

**ap name** *ap-name* **mesh daisy-chaining** [**strict-rap**]

## Syntax Description

| | |
|---|---|
| *ap-name* | Name of the mesh AP. |
| **strict-rap** | Configures to allow only the Ethernet interface as mesh uplink. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

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

### Examples

The following example shows how to configure daisy-chaining mode for a mesh AP:

```
Device# ap name mymeshap mesh daisy-chaining
```

# ap name mesh ethernet mode access

To configure the mode of Ethernet interface as access for a mesh AP, use the **ap name** *ap-name* **mesh ethernet** *port-no* **mode access** command.

**ap name** *ap-name* **mesh ethernet** *port-no* **mode access** *vlan-id*

## Syntax Description

| | |
|---|---|
| *ap-name* | Name of the mesh AP. |
| *port-no* | Port number of the AP. Valid options are 1, 2, 3, and 4. |
| *vlan-id* | VLAN ID. Valid range is from 0 to 4095. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

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

### Examples

The following example shows how to configure the mode of Ethernet interface as access for a mesh AP:

```
Device# ap name mymeshap mesh ethernet 0 mode access 10
```

# ap name mesh ethernet mode trunk

To configure the mode of Ethernet interface as trunk for a mesh AP, use the **ap name** *ap-name* **mesh ethernet** *port-no* **mode trunk** command.

**ap name** *ap-name* **mesh ethernet** *port-no* **mode trunk vlan** {**allowed** | **native**}*vlan-id*

## Syntax Description

| | |
|---|---|
| *ap-name* | Name of the mesh AP. |
| *port-no* | Port number of the AP. Valid options are 1, 2, 3, and 4. |
| **allowed** | Configures allowed VLANs for the trunk port. |
| **native** | Configures native VLAN for the trunk port. |
| *vlan-id* | VLAN ID. Valid range for allowed VLANs is from 0 to 4095. Valid range for native VLANs is 1 to 4095. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

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

### Examples

The following example shows how to configure the mode of Ethernet interface as trunk for a mesh AP and also configure allowed VLANs for the trunk port:

```
Device# ap name mymeshap mesh ethernet 0 mode trunk vlan allowed 10
```

# ap name mesh linktest

To perform a link test with a mesh AP, use the **ap name** *ap-name***mesh linktest** command.

**ap name** *ap-name* **mesh linktest** *dest-ap-mac data-rate pkts-per-sec pkt-size test-duration*

## Syntax Description

| | |
|---|---|
| *ap-name* | Name of the mesh AP. |
| *dest-ap-mac* | MAC address of the destination mesh AP. |
| *data-rate* | Data rate in Mbps (1, 2, 5.5, 6, 9, 11, 12, 24, 36, 48, 53, m0-m15) |
| *pkts-per-sec* | Packets to be sent per second. Valid range is from 1 to 25000. |
| *pkt-size* | Packet size. Valid range is from 1 to 1500. |
| *test-duration* | Test duration. Valid range is from 10 to 300 seconds. |

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

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

### Examples

The following example shows how to configure a link test for a mesh AP:

```
Device# ap name mymeshap mesh linktest 00c0.00a0.03fa.0000.0000.0000
 9 100 10 180
```

# ap name mesh parent preferred

To configure preferred parent for a mesh AP, use the **ap name mesh parent preferred** command.

**ap name** *ap-name* **mesh parent preferred** *mac-address*

## Syntax Description

| | |
|---|---|
| *ap-name* | Name of the mesh AP. |
| *mac-address* | Radio MAC address of the parent AP. |

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

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

### Examples

The following example shows how to preferred parent for a mesh AP:

```
Device # ap name mymeshap mesh parent preferred dc:5f:be:f5:fd:84
```

# ap name mesh security psk provisioning delete

To delete PSK-provisioned key from a mesh AP, use the **ap name mesh security psk provisioning delete** command.

**ap name** *ap-name* **mesh security psk provisioning delete**

## Syntax Description

| | |
|---|---|
| *ap-name* | Name of the mesh AP. |

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

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

### Examples

The following example shows how to delete PSK-provisioned key from a mesh AP:

```
Device# ap name mymeshap mesh security psk provisioning delete
```

# ap name mesh vlan-trunking native

To configure native VLAN for mesh AP, use the **ap name mesh vlan-trunking native** command.

**ap name** *name-of-rap* **vlan-trunking native** *vlan-id*

## Syntax Description

| | |
|---|---|
| *name-of-rap* | Name of the root access point. |
| *vlan-id* | VLAN ID. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

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

### Example

The following example shows how to configure native VLAN for mesh AP:

```
Device # ap name mesh vlan-trunking native 12
```

# ap name mode

To change a Cisco device communication option for an individual Cisco lightweight access point, use the **ap name mode** command.

**ap name** *ap-name* **mode** {**local submode** {**none** | **wips**} | **monitor submode** {**none** | **wips**} | **rogue** | **se-connect** | **sniffer**}

## Syntax Description

| | |
|---|---|
| *ap-name* | Name of the Cisco lightweight access point. |
| **local** | Converts from an indoor mesh access point (MAP or RAP) to a nonmesh lightweight access point (local mode). |
| **submode** | Specifies wIPS submode on an access point. |
| **none** | Disables the wIPS on an access point. |
| **monitor** | Specifies monitor mode settings. |
| **wips** | Enables the wIPS submode on an access point. |
| **rogue** | Enables wired rogue detector mode on an access point. |
| **se-connect** | Enables spectrum expert mode on an access point. |
| **sniffer** | Enables wireless sniffer mode on an access point. |

## Command Default

Local

## Command Modes

Privileged EXEC(#)

## Command History

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

## Usage Guidelines

The sniffer mode captures and forwards all the packets from the clients on that channel to a remote machine that runs AiroPeek or other supported packet analyzer software. It includes information on the timestamp, signal strength, packet size and so on.

This example shows how to set the device to communicate with access point AP01 in local mode:

```
Device# ap name AP01 mode local submode none
```

This example shows how to set the device to communicate with access point AP01 in a wired rogue access point detector mode:

```
Device# ap name AP01 mode rogue
```

This example shows how to set the device to communicate with access point AP02 in wireless sniffer mode:

```
Device# ap name AP02 mode sniffer
```

# ap name mode bridge

To configure Bridge mode for an AP, use the **ap name** *ap-name* **mode bridge** command.

**ap name** *ap-name* **mode bridge**

## Syntax Description

| | |
|---|---|
| *ap-name* | Name of the AP. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

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

### Examples

The following example shows how to configure a Bridge mode for an AP:

```
Device# ap name my-ap mode bridge
```

# ap name monitor-mode

To configure Cisco lightweight access point channel optimization, use the **ap name monitor-mode** command.

**ap name** *ap-name* **monitor-mode** {**no-optimization** | **tracking-opt** | **wips-optimized**}

## Syntax Description

| | |
|---|---|
| *ap-name* | Name of the Cisco lightweight access point. |
| **no-optimization** | Specifies no channel scanning optimization for the access point. |
| **tracking-opt** | Enables tracking optimized channel scanning for the access point. |
| **wips-optimized** | Enables wIPS optimized channel scanning for the access point. |

## Command Default

None

## Command Modes

Privileged EXEC(#)

## Command History

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

This example shows how to configure a Cisco wireless intrusion prevention system (wIPS) monitor mode on access point AP01:

```
Device# ap name AP01 monitor-mode wips
```

# ap name monitor-mode dot11b

To configures 802.11b scanning channels for a monitor-mode access point, use the **ap name monitor-mode dot11b** command.

**ap name** *ap-name* **monitor-mode dot11b fast-channel** *channel1* [*channel2*] [*channel3*] [*channel4*]

## Syntax Description

| | |
|---|---|
| *ap-name* | Name of the access point. |
| **fast-channel** | Specifies the 2.4 GHz band scanning channel (or channels) for a monitor-mode access point. |
| *channel1* | Scanning channel1. |
| *channel2* | (Optional) Scanning channel2. |
| *channel3* | (Optional) Scanning channel3. |
| *channel4* | (Optional) Scanning channel4. |

## Command Default

None

## Command Modes

Privileged EXEC(#)

## Command History

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

This example shows how to configure an access point in tracking optimized mode to listen to channels 1, 6, and 11:

```
Device# ap name AP01 monitor-mode dot11b fast-channel 1 6 11
```

# ap name name

To modify the name of a Cisco lightweight access point, use the **ap name name** command.

**ap name** *ap-name* **name** *new-name*

### Syntax Description

| | |
|---|---|
| *ap-name* | Current Cisco lightweight access point name. |
| *new-name* | Desired Cisco lightweight access point name. |

### Command Default

None

### Command Modes

Privileged EXEC(#)

### Command History

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

This example shows how to modify the name of access point AP1 to AP2:

```
Device# ap name AP1 name AP2
```

# ap name priority

To configure the priority of an access point, use the **ap name priority** command.

**ap name** *ap-name* **priority** *priority-value*

## Syntax Description

| | |
|---|---|
| *priority-value* | Priority value for the AP. Valid range is 1 to 4. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

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

### Examples

The following example shows how to configure the priority for an access point:

```
Device# ap name my-ap priority 1
```

# ap name reset

To reset a specific Cisco lightweight access point, use the **ap name reset** command.

**ap name** *ap-name* **reset**

## Syntax Description

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

## Command Default

None

## Command Modes

Privileged EXEC(#)

## Command History

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

This example shows how to reset a Cisco lightweight access point named AP2:

```
Device# ap name AP2 reset
```

# ap name reset-button

To configure the Reset button for an access point, use the **ap name reset-button** command.

**ap name** *ap-name* **reset-button**

## Syntax Description

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

## Command Default

None

## Command Modes

Privileged EXEC(#)

## Command History

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

This example shows how to enable the Reset button for access point AP03:

```
Device# ap name AP03 reset-button
```

# ap name role

To configure the role of operation for an AP, use the **ap name role** command.

**ap** **name** *ap-name* **role** {**mesh-ap** | **root-ap**}

## Syntax Description

| | |
|---|---|
| *ap-name* | Name of the AP. |
| **mesh-ap** | Configures mesh AP role for the AP. |
| **root-ap** | Configures root AP role for the AP. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

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

### Examples

The following example shows how to configure the role of operation as mesh AP for an AP:

```
Device# ap name mymeshap role mesh-ap
```

# ap name slot

To configure various slot parameters, use the **ap name slot** command. To disable a slot on a Cisco lightweight access point, use the **no** form of this command.

**ap name** *ap-name* **slot** *slot-number* {**channel** {**global** | **number** *channel-number* | **width** *channel-width*} | **rtsthreshold** *value* | **shutdown** | **txpower** {**global***channel-level*}}
**ap name** *ap-name* **no slot** {**0** | **1** | **2** | **3**} **shutdown**

## Syntax Description

| | |
|---|---|
| *ap-name* | Name of the Cisco access point. |
| *slot-number* | Slot downlink radio to which the channel is assigned. You can specify the following slot numbers:<br>• **0**—Enables slot number 0 on a Cisco lightweight access point.<br>• **1**—Enables slot number 1 on a Cisco lightweight access point.<br>• **2**—Enables slot number 2 on a Cisco lightweight access point.<br>• **3**—Enables slot number 3 on a Cisco lightweight access point. |
| **channel** | Specifies the channel for the slot. |
| **global** | Specifies channel global properties for the slot. |
| **number** | Specifies the channel number for the slot. |
| *channel-number* | Channel number from 1 to 169. |
| **width** | Specifies the channel width for the slot. |
| *channel-width* | Channel width from 20 to 40. |
| **rtsthreshold** | Specifies the RTS/CTS threshold for an access point. |
| *value* | RTS/CTS threshold value from 0 to 65535. |
| **shutdown** | Shuts down the slot. |
| **txpower** | Specifies Tx power for the slot. |
| **global** | Specifies auto-RF for the slot. |
| *channel-level* | Transmit power level for the slot from 1 to 7. |

## Command Default

None

## Command Modes

Privileged EXEC(#)

## Command History

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

This example shows how to enable slot 3 for the access point abc:

```
Device# ap name abc slot 3
```

This example shows how to configure RTS for the access point abc:

```
Device# ap name abc slot 3 rtsthreshold 54
```

# ap name static-ip

To configure lightweight access point static IP settings, use the **ap name static-ip** command. To disable the Cisco lightweight access point static IP address, use the **no** form of this command.

**ap name** *ap-name* **static-ip** {**domain** *domain-name* | **ip-address** *ip-address* **netmask** *netmask* **gateway** *gateway* | **nameserver** *ip-address*}
**ap name** *ap-name* **no static-ip**

## Syntax Description

| | |
|---|---|
| *ap-name* | Name of the access point. |
| **domain** | Specifies the Cisco access point domain name. |
| *domain-name* | Domain to which a specific access point belongs. |
| **ip-address** | Specifies the Cisco access point static IP address. |
| *ip-address* | Cisco access point static IP address. |
| **netmask** | Specifies the Cisco access point static IP netmask. |
| *netmask* | Cisco access point static IP netmask. |
| **gateway** | Specifies the Cisco access point gateway. |
| *gateway* | IP address of the Cisco access point gateway. |
| **nameserver** | Specifies a DNS server so that a specific access point can discover the device using DNS resolution. |
| *ip-address* | IP address of the DNS server. |

## Command Default

None

## Command Modes

Privileged EXEC(#)

## Command History

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

## Usage Guidelines

An access point cannot discover the device using Domain Name System (DNS) resolution if a static IP address is configured for the access point unless you specify a DNS server and the domain to which the access point belongs.

This example shows how to configure an access point static IP address:

```
Device# ap name AP2 static-ip ip-address 192.0.2.54 netmask 255.255.255.0 gateway 192.0.2.1
```

# ap name shutdown

To disable a Cisco lightweight access point, use the **ap name shutdown** command. To enable a Cisco lightweight access point, use the **no** form of this command.

**ap name** *ap-name* **shutdown**
**ap name** *ap-name* **no shutdown**

## Syntax Description

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

## Command Default

None

## Command Modes

Privileged EXEC(#)

## Command History

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

This example how to disable a specific Cisco lightweight access point:

```
Device# ap name AP2 shutdown
```

# ap name sniff

To enable sniffing on an access point, use the **ap name sniff** command. To disable sniffing on an access point, use the **no** form of this command.

**ap name** *ap-name* **sniff** { **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 Omnipeek, Airopeek, AirMagnet, or Wireshark software. |

## Command Default

Channel 36

## Command Modes

Privileged EXEC(#)

## Command History

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

## Usage Guidelines

When the sniffer feature is enabled on an access point, it starts sniffing the signal on the given channel. It captures and forwards all the packets to the remote computer that runs Omnipeek, Airopeek, AirMagnet, or Wireshark software. It includes information about the timestamp, signal strength, packet size and so on.

Before an access point can act as a sniffer, a remote computer that runs one of the listed packet analyzers must be set up so that it can receive packets that are sent by the access point.

This example shows how to enable the sniffing on the 5 GHz band for an access point on the primary wireless LAN controller:

```
Device# ap name AP2 sniff dot11a 36 192.0.2.54
```

# ap name tftp-downgrade

To configure the settings used for downgrading a lightweight access point to an autonomous access point, use the **ap name tftp-downgrade** command.

**ap name** *ap-name* **tftp-downgrade** *tftp-server-ip* *filename*

## Syntax Description

| | |
|---|---|
| *ap-name* | Name of the Cisco lightweight access point. |
| *tftp-server-ip* | IP address of the TFTP server. |
| *filename* | Filename of the access point image file on the TFTP server. |

## Command Default

None

## Command Modes

Privileged EXEC(#)

## Command History

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

This example shows how to configure the settings for downgrading access point AP1:

```
Device# ap name Ap01 tftp-downgrade 172.21.12.45 ap3g1-k9w7-tar.124-25d.JA.tar
```

# ap name vlan-tag

To configure VLAN tagging for a nonbridge AP, use the **ap name vlan-tag** command.

**ap name** *ap-name* **vlan-tag** *vlan-id*

## Syntax Description

| | |
|---|---|
| *ap-name* | Access point name. |
| *vlan-id* | VLAN identifier. |

## Command Default

VLAN tagging is not enabled.

## Command Modes

Privileged EXEC

## Command History

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

### Example

The following example shows how to configure VLAN tagging for a nonbridge AP:

```
Device# ap name AP1 vlan-tag 12
```

# ap name write tag-config

To write the existing configuration to an AP, use the **ap name write tag-config** command in privileged EXEC mode

**ap name** *ap-name***write tag-config**

## Syntax Description

| | |
|---|---|
| *ap-name* | Name of the access point. |

## Command Default

None

## Command Modes

Privileged EXEC(#)

## Command History

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

## Usage Guidelines

Use this command to write the existing configuration to an AP.

### Example

This example shows how to write the existing configuration to an AP:

```
Device# ap name AP40CE.2485.D594 write tag-config
```

# ap name-regex

To configure filter based on AP name regular expression to match with, use the **ap name-regex** command.

**ap name-regex** *regular-expression*

## Syntax Description

| | |
|---|---|
| *regular-expression* | Enter the filter string. |

## Command Default

None

## Command Modes

Privileged EXEC(#)

## Command History

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

### Examples

The following example shows how to configure filter based on AP name regular expression match with:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap filter name filter--name
Device(config-ap-filter)# ap name-regex regular-expression-string
```

# ap packet-capture

To start or stop the AP packet capture process, use the **ap packet-capture** command.

**ap packet-capture** {**start** | **stop**} *client-mac-address* {**auto** | **static** *ap-name*}

## Syntax Description

| | |
|---|---|
| *client-mac-address* | Client MAC address. |
| *ap-name* | AP name. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

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

## Usage Guidelines

When using the **stop** option with **ap packet capture** command, use the keyword **all** to stop the packet capture.

### Example

The following example shows how to start the AP packet capture process:

```
Device# ap packet-capture start 3c08.f672.1ad9 static AP_2029
```

The following example shows how to stop the AP packet capture process fully:

```
Device# ap packet-capture stop 3c08.f672.1ad9 all
```

# ap packet-capture profile

To configure the AP packet capture profile, use the **ap packet-capture profile**command.

**ap packet-capture profile** *profile-name*

## Syntax Description

| | |
|---|---|
| *profile-name* | AP packet capture profile name. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

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

### Example

The following example shows how to configure the AP packet capture profile:

```
Device# ap packet-capture profile test1
```

# ap packet-capture start

To enables packet capture for the specified client on a set of nearby access points, use the **ap packet-capture start** command.

**ap packet-capture start** *client-mac-addr* {**auto** | **static** *ap-name*}

## Syntax Description

| | |
|---|---|
| *client-mac-addr* | MAC address of the client whose packet capture has to be done. |
| **auto** | Starts packet capture in the nearby APs. |
| **static** *ap-name* | Name of the AP in which the packet capture has to be done. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

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

### Examples

The following example shows how to enable packet capture for a client on a set of nearby access points:

```
Device# ap packet-capture start 0011.0011.0011 auto
```

# ap profile

To configure access point profile, use the **ap profile** command.

**ap profile** *profile-name*

## Syntax Description

| | |
|---|---|
| *profile-name* | Enter the name of the AP profile. |

## Command Default

By default, the AP profile name is default-ap-profile.

## Command Modes

Global configuration (config)

## Command History

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

### Examples

The following example shows how to configure AP profile name:

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

# ap remote-lan profile-name

To configure remote LAN profile, use the **ap remote-lan profile-name** command.

**ap remote-lan profile-name** *remote-lan-profile-name rlan-id*

## Syntax Description

| | |
|---|---|
| **remote-lan-profile-name** | Is the remote LAN profile name. Range is from 1 to 32 alphanumeric characters. |
| **rlan-id** | Is the remote LAN identifier. Range is from 1 to 128.<br>**Note** You can create a maximum of 128 RLANs. You cannot use the *rlan-id* of an existing RLAN while creating another RLAN.<br>Both RLAN and WLAN profile cannot have the same names. Similarly, RLAN and WLAN policy profile cannot have the same names. |

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

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

This example shows how to configure remote LAN profile:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap remote-lan profile-name rlan_profile_name 3
```

# ap remote-lan shutdown

To enable or disable all RLANs, use the **ap remote-lan shutdown** command.

**ap remote-lan shutdown**

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

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

### Example

This example shows how to enable or disable all RLANs:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# [no] ap remote-lan shutdown
Device(config)# end
```

# ap remote-lan-policy policy-name

To configure RLAN policy profile, use the **ap remote-lan-policy policy-name** command.

**ap remote-lan-policy policy-name** *profile-name*

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

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

### Example

This example shows how to configure RLAN policy profile:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap remote-lan-policy policy-name rlan_policy_prof_name
```

# ap upgrade staggered iteration timeout

To configure the maximum time allowed per iteration during an access point (AP) upgrade, use the **ap upgrade staggered iteration timeout** command.

**ap upgrade staggered iteration timeout** *timeout-duration*

## Syntax Description

| | |
|---|---|
| *timeout-duration* | Time allowed per iteration, in minutes.<br>Valid values range from 9 to 60. |

## Command Default

Iteration timeout is not configured.

## Command Modes

Global configuration (config)

## Command History

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

## Usage Guidelines

If an AP upgrade iteration is not completed during the specified duration, the error action that is set using the **ap upgrade staggered iteration error** command is taken.

## Examples

The following example shows how to configure the maximum time allowed per iteration:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap upgrade staggered iteration timeout 40
```

# ap tag-source-priority

To configure ap tag source priority, use the **ap tag-source-priority** command.

**ap tag-source-priority** *source-priority* **source** { **filter** | **ap** }

## Syntax Description

| | |
|---|---|
| *source-priority* | Enter the ap tag source priority. Valid range is 2 to 3. |
| **source** | Specifiy the source for which priority is been set. |
| **filter** | AP filter as tag source. |
| **ap** | AP as tag source. |

## Command Default

None

## Command Modes

config

## Command History

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

### Examples

The following example shows how to set AP as a tag source:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap tag-source-priority priority-value source ap
```

# ap tag-sources revalidate

To revalidate the access point tag sources, use the **ap tag-sources revalidate** command.

**ap tag-sources revalidate**

## Syntax Description

| | |
|---|---|
| **tag-sources** | Tag Sources. |
| **revalidate** | Revalidate access point tag sources. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

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

### Examples

The following example shows how to revalidate the access point tag sources:

```
Device# ap tag-sources revalidate
```

# ap vlan-tag

To configure VLAN tagging for all nonbridge APs, use the **ap vlan-tag** command.

**ap vlan-tag** *vlan-id*

## Syntax Description

| | |
|---|---|
| *vlan-id* | VLAN identifier. |

## Command Default

VLAN tagging is not enabled for nonbridge APs.

## Command Modes

Privileged EXEC

## Command History

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

### Example

The following example shows how to configure VLAN tagging for all non-bridge APs:

```
Device# ap vlan-tag 1000
```

# arp-caching

To enable arp-caching, use the **arp-caching** command.

**arp-caching**

## Syntax Description

This command has no keywords or arguments.

## Command Default

None

## Command Modes

config-wireless-flex-profile

## Command History

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

### Example

The following example shows how to enable arp-caching:

```
Device(config-wireless-flex-profile)# arp-caching
```

# assisted-roaming

To configure assisted roaming using 802.11k on a WLAN, use the **assisted-roaming** command. To disable assisted roaming, use the **no** form of this command.

**assisted-roaming** {**dual-list** | **neighbor-list** | **prediction**}

**no assisted-roaming** {**dual-list** | **neighbor-list** | **prediction**}

## Syntax Description

| | |
|---|---|
| **dual-list** | Configures a dual band 802.11k neighbor list for a WLAN. The default is the band that the client is currently associated with. |
| **neighbor-list** | Configures an 802.11k neighbor list for a WLAN. |
| **prediction** | Configures assisted roaming optimization prediction for a WLAN. |

## Command Default

Neighbor list and dual band support are enabled by default. The default is the band that the client is currently associated with.

## Command Modes

WLAN configuration

## Usage Guidelines

When you enable the assisted roaming prediction list, a warning appears and load balancing is disabled for the WLAN if load balancing is already enabled on the WLAN. To make changes to the WLAN, the WLAN must be in disabled state.

### Example

The following example shows how to configure a 802.11k neighbor list on a WLAN:

```
Device(config-wlan)#assisted-roaming neighbor-list
```

The following example shows the warning message when load balancing is enabled on a WLAN. Load balancing must be disabled if it is already enabled when configuring assisted roaming:

```
Device(config)#wlan test-prediction 2 test-prediction
Device(config-wlan)#client vlan 43
Device(config-wlan)#no security wpa
Device(config-wlan)#load-balance
Device(config-wlan)#assisted-roaming prediction
WARNING: Enabling neighbor list prediction optimization may slow association and impact
VOICE client perform.
Are you sure you want to continue? (y/n)[y]: y
% Request aborted - Must first disable Load Balancing before enabling Assisted Roaming
Prediction Optimization on this WLAN.
```

# autoqos

To enable Auto QoS wireless policy, use the **autoqos** command. To remove Auto QoS wireless policy, use the **no** form of this command.

**autoqos mode** { **enterprise-avc** | **fastlane** | **guest** | **voice** }

## Syntax Description

| | |
|---|---|
| **enterprise-avc** | Enables AutoQos wireless Enterprise policy. |
| **fastlane** | Enable AutoQos wireless fastlane policy. |
| **guest** | Enables AutoQos wireless guest policy |
| **voice** | Enables AutoQos wireless voice policy |

## Command Default

None

## Command Modes

Wireless policy configuration

## Command History

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

This example shows how to enable AutoQos Wireless Enterprise Policy.

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

# avg-packet-size packetsize

To configure the wireless media-stream's average packet size, use the **avg-packet-size** command.

**avg-packet-size** *packetsize-value*

## Syntax Description

| | |
|---|---|
| *packetsize-value* | Average Packet Size. Valid range is 100 to 1500. |

## Command Default

None

## Command Modes

media-stream

## Command History

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

### Examples

The following example shows how to configure wireless media-stream's average packet size:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless media-stream group doc-grp 224.0.0.0 224.0.0.223
Device(config-media-stream)# avg-packet-size500
```

# 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

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

### Example

The following example shows how to configure mesh backhaul details for a mesh AP profile:

```
Device # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device (config)# wireless profile mesh mesh-profile
Device (config-wireless-mesh-profile)# backhaul rate dot11 24ghz auto
```

# background-scanning (mesh)

To configure background scanning for a mesh AP profile, use the **background-scanning** command.

**background-scanning**

## Syntax Description

This command has no keywords or arguments.

## Command Default

Background scanning is disabled.

## Command Modes

config-wireless-mesh-profile

## Command History

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

### Example

The following example shows how to configure background scanning for a mesh AP profile:

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

# band-select client

To configure the client threshold minimum dB for the selected band, use the **band-select client** command. To reset the client threshold minimum dB for the selected band, use the **no** form of this command.

**band-select client** {**mid-rssi** | **rssi** } *dBm value*

## Syntax Description

| | |
|---|---|
| **mid-rssi** | Minimum dBm of a client RSSI start to respond to probe |
| **rssi** | Minimum dBm of a client RSSI to respond to probe |
| *dBm value* | Minimum dBm of a client RSSI to respond to probe. Valid range is between –90 and –20 dBm. |

## Command Default

None

## Command Modes

config-rf-profile

## Command History

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

## Usage Guidelines

This command is enabled only for 2.4-GHz band.

This example shows how to set the client threshold to minimum dB for a selected band.

```
Device(config-rf-profile)#band-select client rssi -50
```

# band-select cycle

To configure the band cycle parameters, use the **band-select cycle** command. To reset the threshold value, use the **no** form of this command.

**band-select cycle** { **count** | **threshold** } *value*

## Syntax Description

| | |
|---|---|
| **count** | Sets the Band Select probe cycle count. |
| *value* | Maximum number of cycles not responding. The range is between 1 and 10. |
| **threshold** | Sets the time threshold for a new scanning cycle. |
| *value* | Set the threshold value in milliseconds. The valid is between 1and 1000. |

## Command Default

None

## Command Modes

config-rf-profile

## Command History

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

## Usage Guidelines

None

This example shows how to configure the probe cycle count in an RF profile for a selected band.

```
Device(config-rf-profile)#band-select cycle count 5
```

# band-select expire

To configure the expiry time for the RF profile for the selected band, use the **band-select expire** command. To reset the value, use the **no** form of this command.

**band-select expire** { **dual-band** | **suppression** } *value*
**no band-select expire** { **dual-band** | **suppression** }

## Syntax Description

| | |
|---|---|
| **dual-band** | Configures the RF Profile Band Select Expire Dual Band. |
| *value* | Setting the time to expire for pruning previously known dual-band clients. The range is between 10 and 300. |
| **suppression** | Configures the RF Profile Band Select Expire Suppression. |
| *value* | Setting the time to expire for pruning previously known 802.11b/g clients. The range is between 10 and 200. |

## Command Default

None

## Command Modes

config-rf-profile

## Command History

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

## Usage Guidelines

None

This example shows how to configure the time to expire for a dual-band of an RF profile in a selected band.

```
Device(config-rf-profile)#band-select expire dual-band 15
```

# band-select probe-response

To configure the probe responses to the clients for a selected band, use the **band-select probe-response** command. To disable the probe-response, use the **no** form of this command.

**band-select probe-response**

## Syntax Description

| | |
|---|---|
| **probe-response** | Probe responses to clients. |

## Command Default

None

## Command Modes

config-rf-profile

## Command History

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

## Usage Guidelines

None

This example shows how to enable probe response to the clients.

```
Device(config-rf-profile)#band-select probe-response
```

# banner text

To configure the message in a banner, use the **banner text** command. Use the **no** form of this command to remove the message.

**banner text** *text*

**no banner text**

## Syntax Description

| | |
|---|---|
| *text* | Text message to be displayed. |

## Command Default

None

## Command Modes

Parameter map configuration

## Command History

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

## Examples

The following example shows how to configure a message in a banner:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# parameter-map type webauth global
Device(config-params-parameter-map)# banner text #Hêllö#
```

# battery-state (mesh)

To configure battery state for an AP, use the **battery-state** command.

**battery-state**

## Syntax Description

This command has no keywords or arguments.

## Command Default

Battery state is enabled.

## Command Modes

config-wireless-mesh-profile

## Command History

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

### Example

The following example shows how to configure battery state for an AP:

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

# bridge-group

To configure bridge group parameters for a mesh AP profile, use the **bridge-group** command.

**bridge-group** {**name** *bridge-group-name* | **strict-match** }

## Syntax Description

| | |
|---|---|
| **name** *bridge-group-name* | Configures bridge group name. |
| **strict-match** | Configures bridge group strict matching. |

## Command Default

None

## Command Modes

config-wireless-mesh-profile

## Command History

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

### Examples

The following example shows how to configure the bridge group name for a mesh AP profile:

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

# bss-transition

To configure BSS transition per WLAN, use the **bss-transition** command.

**bss-transition** [**disassociation-imminent**]

## Syntax Description

| | |
|---|---|
| **disassociation-imminent** | BSS transition disassociation Imminent per WLAN. |

## Command Default

None

## Command Modes

config-wlan

## Command History

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

### Example

The following example shows how to configure BSS transition per WLAN:

```
Device(config-wlan)# bss-transition
```

# cache timeout active value

To set the active flow monitor timeout value in seconds, use the **cache timeout active value** command.

**cache timeout active** *value*

## Syntax Description

| | |
|---|---|
| *value* | Enter the active timeout value. Valid range is 1 to 604800. |

## Command Default

None

## Command Modes

config-flow-monitor

## Command History

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

### Examples

The following example shows how to set the flow monitor inactive timeout value:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# flow monitor flow-monitor-name
Device(config-flow-monitor)# cache timeout active 300
```

# cache timeout inactive value

To set the flow monitor inactive timeout value in seconds, use the **cache timeout inactive value** command.

**cache timeout inactive** *value*

## Syntax Description

| | |
|---|---|
| *value* | Enter the inactive timeout value. Valid range is 1 to 604800. |

## Command Default

None

## Command Modes

config-flow-monitor

## Command History

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

### Examples

The following example shows how to set the flow monitor inactive timeout value:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# flow monitor flow-monitor-name
Device(config-flow-monitor)# cache timeout inactive 300
```

# call-snoop

**call-snoop**

**no call-snoop**

## Syntax Description

This command has no keywords or arguments.

## Command Default

VoIP snooping is disabled by default.

## Command Modes

WLAN configuration

## Command History

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

## Usage Guidelines

You must disable the WLAN before using this command. The WLAN on which call snooping is configured must be configured with Platinum QoS. You must disable quality of service before using this command.

### Example

This example shows how to enable VoIP on a WLAN:

```
Device# configure terminal
Device(config)# wireless profile policy policy-name
Device(config-wireless-policy)#service-policy input platinum-up
Device(config-wireless-policy)#service-policy output platinum
Device(config-wireless-policy)#call-snoop
Device(config-wireless-policy)#no shutdown
Device(config-wireless-policy)#end
```

# captive-bypass-portal

To configure captive bypassing, use the **captive-bypass-portal** command.

**captive-bypass-portal**

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

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

### Example

This example shows how to configure captive bypassing for WLAN in LWA and CWA:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# parameter-map type webauth WLAN1_MAP
Device(config)# captive-bypass-portal
Device(config)# wlan WLAN1_NAME 4 WLAN1_NAME
Device(config-wlan)# security web-auth
Device(config-wlan)# security web-auth parameter-map WLAN1_MAP
Device(config-wlan)# end
```

# capwap-discovery

To set CAPWAP discovery response method as to whether a capwap-discovery response contains the public or private IP of the controller, use the **capwap-discovery** command.

**capwap-discovery** {**private** | **public**}

## Syntax Description

| | |
|---|---|
| **private** | Includes private IP in CAPWAP discovery response. |
| **public** | Includes public IP in CAPWAP discovery response. |

## Command Default

None

## Command Modes

Management Interface Configuration(config-mgmt-interface)

## Command History

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

## Usage Guidelines

### Example

The following example shows how to configure a CAPWAP discovery response method:

```
Device# configure terminal
Device(config)# wireless management interface Vlan1
Device(config-mgmt-interface)# capwap-discovery public
```

# capwap backup

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

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

## Syntax Description

| | |
|---|---|
| **primary** | Specifies the primary backup device. |
| *primary-controller-name* | Primary backup device name. |
| *primary-controller-ip-address* | Primary backup device IP address. |
| **secondary** | Specifies the secondary backup device. |
| *secondary-controller-name* | Secondary backup device name. |
| *secondary-controller-ip-address* | Secondary backup device IP address. |

## Command Default

None

## Command Modes

AP profile configuration (config-ap-profile)

## Command History

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

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

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

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

```
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# capwap backup secondary controller1 192.0.2.52
```

# ccn (mesh)

To configure channel change notification for a mesh AP profile, use the **ccn** command.

**ccn**

## Syntax Description

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

## Command Default

Channel change notification is disabled.

## Command Modes

config-wireless-mesh-profile

## Command History

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

### Example

The following example shows how to configure channel change notification for a mesh AP profile:

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

# cdp

To enable the Cisco Discovery Protocol (CDP) on a Cisco lightweight access point under the AP profile, use the **cdp** command. To disable the Cisco Discovery Protocol (CDP) on a Cisco lightweight access point, use the **no** form of this command.

```
ap profile default-ap-profile

cdp
```

**no cdp**

## Command Default

Disabled on all access points.

## Command Modes

AP profile mode (config-ap-profile)

## Command History

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

## Usage Guidelines

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

**Note** CDP over Ethernet/radio interfaces is available only when CDP is enabled.

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

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


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

# central 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

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

### 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.

**central authentication**

## Syntax Description

This command has no keywords or arguments.

## Command Default

None

## Command Modes

config-wireless-policy

## Command History

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

### Example

The following example shows how to enable central authentication:

```
Device(config-wireless-policy)# central authentication
```

# central dhcp

To enable central dhcp for locally switched clients, use the **central dhcp** command.

**central dhcp**

## Syntax Description

This command has no keywords or arguments.

## Command Default

None

## Command Modes

config-wireless-policy

## Command History

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

### Example

The following example shows how to enable central dhcp for locally switched clients:

```
Device(config-wireless-policy)# central dhcp
```

# central switching

To enable or disable central switching, use the **central switching** command.

**central switching**

## Syntax Description

This command has no keywords or arguments.

## Command Default

None

## Command Modes

config-wireless-policy

## Command History

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

### Example

The following example shows how to enable or disable central switching:

```
Device(config-wireless-policy)# central switching
```

# central-webauth

To configure central-webauth for an ACL, use the **central-webauth** command.

**central-webauth**

## Syntax Description

This command has no keywords or arguments.

## Command Default

None

## Command Modes

config-wireless-policy

## Command History

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

### Example

The following example shows how to configure central-webauth for an ACL:

```
Device(config-wireless-policy)# central-webauth
```

# chassis redundancy ha-interface

To configure the high availability (HA) interface for a chassis, use the **chassis redundancy ha-interface** command.

**chassis redundancy ha-interface GigabitEthernet***interface-number* **local-ip** *ip-address netmask* **remote-ip** *remote-chassis-ip-addr*

## Syntax Description

| | |
|---|---|
| *interface-number* | GigabitEthernet interface number. Valid range is 1 to 32. |
| **local-ip** *ip-address netmask* | Configures the IP address of the local chassis HA interface. For the netmask, enter the netmask or the prefix length in the following formats: */nn* or *A.B.C.D*. |
| **remote-ip** *remote-chassis-ip-addr* | Configures the remote chassis IP address. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

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

### Examples

The following example shows how to configure the HA interface for a chassis:

```
Device# chassis ha-interface GigabitEthernet 2 local-ip 10.10.10.10 255.255.255.0 remote-ip
 10.10.10.11
```

# chassis redundancy keep-alive

To configure peer keep-alive retries and time interval before claiming peer is down, use the **chassis redundancy keep-alive** command.

**chassis redundancy keep-alive** { **retries** *retries* | **timer** *timer* }

## Syntax Description

| | |
|---|---|
| *retries* | Chassis peer keep-alive retries before claiming peer is down.<br>Valid values range from 5 to 10, enter 5 for default. |
| *timer* | Chassis peer keep-alive time interval in multiple of 100 ms.<br>Valid values range from 1 to 10, enter 1 for default. |

## Command Default

None

## Command Modes

Privileged EXEC(#)

## Command History

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

### Examples

The following example shows how to configure peer keep-alive retries and time interval:

```
Device# chassis redundancy keep-alive retries 6
```

```
Device# chassis redundancy keep-alive timer 6
```

# chassis renumber

To renumber the local chassis id assignment, use the **chassis renumber** command.

**chassis** *chassis-num* **renumber** *renumber-id*

### Syntax Description

| | |
|---|---|
| *chassis-num* | Chassis number. |
| *renumber-id* | Local chassis id. |

### Command Default

None

### Command Modes

Privileged EXEC(#)

### Command History

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

### Examples

The following example shows how to renumber the local chassis id assignment:

```
Device# chassis 1 renumber 1
```

# chassis priority

To set the priority of the specified device, use the **chassis priority** command.

**chassis** *chassis-num* **priority** *priority-id*

## Syntax Description

| | |
|---|---|
| *chassis-num* | Chassis number. |
| *priority-id* | Chassis priority. |

## Command Default

None

## Command Modes

Privileged EXEC(#)

## Command History

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

### Examples

The following example shows how to set the priority of the specified device:

```
Device# chassis 1 priority 1
```

# chassis transport

To enable or disable chassis transport, use the **chassis transport** command.

**chassis** *chassis-num* **transport** {**enable** | **disable**}

## Syntax Description

| | |
|---|---|
| *chassis-num* | Chassis number. |

## Command Default

None

## Command Modes

Privileged EXEC(#)

## Command History

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

### Examples

The following example shows how to enable chassis transport:

```
Device# chassis 1 transport enable
```

# class

To define a traffic classification match criteria for the specified class-map name, use the **class** command in policy-map configuration mode. Use the **no** form of this command to delete an existing class map.

**class** {*class-map-name* | **class-default**}
**no class** {*class-map-name* | **class-default**}

## Syntax Description

| | |
|---|---|
| *class-map-name* | The class map name. |
| **class-default** | Refers to a system default class that matches unclassified packets. |

## Command Default

No policy map class-maps are defined.

## Command Modes

Policy-map configuration

## Command History

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

## Usage Guidelines

Before using the **class** command, you must use the **policy-map** global configuration command to identify the policy map and enter policy-map configuration mode. After specifying a policy map, you can configure a policy for new classes or modify a policy for any existing classes in that policy map. You attach the policy map to a port by using the **service-policy** interface configuration command.

After entering the **class** command, you enter the policy-map class configuration mode. These configuration commands are available:

- **admit**—Admits a request for Call Admission Control (CAC)
- **bandwidth**—Specifies the bandwidth allocated to the class.
- **exit**—Exits the policy-map class configuration mode and returns to policy-map configuration mode.
- **no**—Returns a command to its default setting.
- **police**—Defines a policer or aggregate policer for the classified traffic. The policer specifies the bandwidth limitations and the action to take when the limits are exceeded. For more information about this command, see *Cisco IOS Quality of Service Solutions Command Reference* available on Cisco.com.
- **priority**—Assigns scheduling priority to a class of traffic belonging to a policy map.
- **queue-buffers**—Configures the queue buffer for the class.
- **queue-limit**—Specifies the maximum number of packets the queue can hold for a class policy configured in a policy map.
- **service-policy**—Configures a QoS service policy.
- **set**—Specifies a value to be assigned to the classified traffic. For more information, see set, on page 555
- **shape**—Specifies average or peak rate traffic shaping. For more information about this command, see *Cisco IOS Quality of Service Solutions Command Reference* available on Cisco.com.

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

The **class** command performs the same function as the **class-map** global configuration command. Use the **class** command when a new classification, which is not shared with any other ports, is needed. Use the **class-map** command when the map is shared among many ports.

You can configure a default class by using the **class class-default** policy-map configuration command. Unclassified traffic (traffic that does not meet the match criteria specified in the traffic classes) is treated as default traffic.

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

## Examples

This example shows how to create a policy map called policy1. When attached to the ingress direction, it matches all the incoming traffic defined in class1, sets the IP Differentiated Services Code Point (DSCP) to 10, and polices the traffic at an average rate of 1 Mb/s and bursts at 20 KB. Traffic exceeding the profile is marked down to a DSCP value gotten from the policed-DSCP map and then sent.

```
Device(config)# policy-map policy1
Device(config-pmap)# class class1
Device(config-pmap-c)# set dscp 10
Device(config-pmap-c)# police 1000000 20000 conform-action
Device(config-pmap-c)# police 1000000 20000 exceed-action
Device(config-pmap-c)# exit
```

This example shows how to configure a default traffic class to a policy map. It also shows how the default traffic class is automatically placed at the end of policy-map pm3 even though **class-default** was configured first:

```
Device# configure terminal
Device(config)# class-map cm-3
Device(config-cmap)# match ip dscp 30
Device(config-cmap)# exit

Device(config)# class-map cm-4
Device(config-cmap)# match ip dscp 40
Device(config-cmap)# exit

Device(config)# policy-map pm3
Device(config-pmap)# class class-default
Device(config-pmap-c)# set dscp 10
Device(config-pmap-c)# exit

Device(config-pmap)# class cm-3
Device(config-pmap-c)# set dscp 4
Device(config-pmap-c)# exit

Device(config-pmap)# class cm-4
Device(config-pmap-c)# set precedence 5
Device(config-pmap-c)# exit
Device(config-pmap)# exit

Device# show policy-map pm3
Policy Map pm3
  Class cm-3
    set dscp 4
  Class cm-4
    set precedence 5
```

```
Class class-default
  set dscp af11
```

# classify

To classify a rule for rogue devices, use the **classify** command.

**classify** {**friendly** | **malicious** | **delete**}

## Syntax Description

| | |
|---|---|
| **friendly** | Classifies devices matching this rule as friendly. |
| **malicious** | Classifies devices matching this rule as malicious. |
| **delete** | Devices matching this rule are ignored. |

## Command Default

None

## Command Modes

config-rule

## Command History

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

### Examples

The following example shows how to classify rogue devices as friendly:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless wps rogue rule my-rogue-rule priority 3
Device(config-rule)# classify friendly
```

# class-map

To create a class map to be used for matching packets to the class whose name you specify and to enter class-map configuration mode, use the **class-map** command in global configuration mode. Use the **no** form of this command to delete an existing class map and to return to global or policy map configuration mode.

**class-map** [**match-any***type*][**match-all***type*] *class-map-name*
**no class-map** [**match-any***type*][**match-all***type*] *class-map-name*

## Syntax Description

| | |
|---|---|
| **match-any** | (Optional) Performs a logical-OR of the matching statements under this class map. One or more criteria must be matched. |
| **type** | (Optional) Configures the CPL class map. |
| *class-map-name* | The class map name. |

## Command Default

No class maps are defined.

## Command Modes

Global configuration

Policy map configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |
| | The **type** keyword was added. |

## Usage Guidelines

Use this command to specify the name of the class for which you want to create or modify class-map match criteria and to enter class-map configuration mode.

The **class-map** command and its subcommands are used to define packet classification, marking, and aggregate policing as part of a globally named service policy applied on a per-port basis.

After you are in quality of service (QoS) class-map configuration mode, these configuration commands are available:

- **description**—Describes the class map (up to 200 characters). The **show class-map** privileged EXEC command displays the description and the name of the class map.
- **exit**—Exits from QoS class-map configuration mode.
- **match**—Configures classification criteria.
- **no**—Removes a match statement from a class map.

If you enter the **match-any** keyword, you can only use it to specify an extended named access control list (ACL) with the **match access-group** class-map configuration command.

To define packet classification on a physical-port basis, only one **match** command per class map is supported.

The ACL can have multiple access control entries (ACEs).

## Examples

This example shows how to configure the class map called class1 with one match criterion, which is an access list called 103:

```
Device(config)# access-list 103 permit ip any any dscp 10
Device(config)# class-map class1
Device(config-cmap)# match access-group 103
Device(config-cmap)# exit
```

This example shows how to delete the class map class1:

```
Device(config)# no class-map class1
```

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

# clear aaa counters servers radius

To clear all AAA server radius or specific server radius, use the **clear aaa counters servers radius** {*server-id* | **all**}

**clear aaa counters servers radius** { *server-id* | **all** }

## Syntax Description

| | |
|---|---|
| *server-id* | Specifies the server IDs of the AAA servers that are displayed by the **show** command. |
| **all** | Specifies all the AAA server IDs. |

## Command Default

None

## Command Modes

Privileged EXEC(#)

## Command History

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

### Example

The following example shows how to clear all AAA server radius:

```
Device# clear aaa counters servers radius all
```

# clear chassis redundancy

To clear high-availability (HA) configuration, use the **clear chassis redundancy** command.

**clear chassis redundancy**

## Syntax Description

This command has no keywords or arguments.

## Command Default

None

## Command Modes

Privileged EXEC(#)

## Command History

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

### Examples

The following example shows how to clear HA configuration:

```
Device# clear chassis redundancy
```

# clear ip nbar protocol-discovery wlan

To clear the NBAR2 protocol discovery statistics on a specific WLAN, use the **clear ip nbar protocol-discovery wlan** command.

**clear ip nbar protocol-discovery wlan** *wlan-name*

## Syntax Description

| | |
|---|---|
| *wlan-name* | Enter the WLAN name. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

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

### Examples

The following example shows how to clear the NBAR protocol discovery statistics on a perticular WLAN:

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

# clear mdns-sd statistics

To clear mDNS statistics, use the **clear mdns-sd statistics** command.

**clear mdns-sd statistics** { **debug** | **glan-id** *<1 - 5>* | **rlan-id** *<1 - 128>* **wired** | **wlan-id** *<1 - 4096>* }

## Syntax Description

| | |
|---|---|
| **debug** | Clears the mDNS debug statistics. |
| **glan-id***<1 - 5>* | Clears the GLAN ID. The value range is from 1 to 5. |
| **rlan-id***<1 - 128>* | Clears the RLAN ID. The value range is from 1 to 128. |
| **wired** | Clears the mDNS wired statistics. |
| **wlan-id***<1 - 4096>* | Clears the WLAN ID. The value range is from 1 to 4096. |

## Command Default

None

## Command Modes

Privileged EXEC mode

## Command History

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

## Usage Guidelines

None

### Example

The following example shows how to clear the mDNS statistics:

```
Device# clear mdns-sd statistics
```

# clear platform condition all

To clear all conditional debug and packet-trace configuration and data, use the **clear platform condition all** command.

**clear platform condition all**

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

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

### Examples

The following example shows how to clear all conditional debug and packet-trace configuration and data:

```
Device# clear platform condition all
```

# clear radius statistics

To clear the radius server information statistics, use the **clear radius statistics** command.

**clear radius statistics**

## Syntax Description

There are no arguments for this command.

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

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

### Example

The following example shows how to clear the radius server information statistics:

```
Device# clear radius statistics
```

# clear subscriber policy peer

To clear the display of the details of a subscriber policy peer connection, use the **clear subscriber policy peer**command in privileged EXEC mode.

**clear subscriber policy peer** {**address** *ip-address* | **handle** *connection-handle-id* | **session** | **all**}

## Syntax Description

| | |
|---|---|
| **address** | Clears the display of a specific peer connection, identified by its IP address. |
| *ip-address* | IP address of the peer connection to be cleared. |
| **handle** | Clears the display of a specific peer connection, identified by its handle. |
| *connection-handle-id* | Handle ID for the peer connection handle. |
| **session** | Clears the display of sessions with the given peer. |
| **all** | Clears the display of all peer connections. |

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SRC | This command was introduced. |
| 12.2(33)SB | This command was integrated into Cisco IOS Release 12.2(33)SB |

## Usage Guidelines

The **clear subscriber policy peer** command ends the peering relationship between the Intelligent Services Gateway (ISG) device and selected Service Control Engine (SCE) devices. However, the SCE will attempt to reconnect with the ISG device after a configured amount of time. The **clear subscriber policy peer** command can remove select session associations from a particular SCE device.

## Examples

The following example shows how the **clear subscriber policy peer**command is used at the router prompt to clear the display of all details of the subscriber policy peer connection.

```
Router# clear subscriber policy peer all
```

## Related Commands

| Command | Description |
|---|---|
| **show subscriber-policy peer** | Displays the details of a subscriber policy peer. |
| **subscriber-policy** | Defines or modifies the forward and filter decisions of the subscriber policy. |

# clear wireless wps rogue ap

To clear all rogue APs or rogue APs with specific MAC addresses, use the **clear wireless wps rogue ap** command.

**clear wireless wps rogue ap** { **all** | **mac-address** *<MAC Address>* }

## Syntax Description

| | |
|---|---|
| **all** | Clears all the rogue APs. |
| **mac-address** *<MAC Address>* | Clears the rogue APs with specific MAC addresses. |

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Amsterdam 16.12.1 | This command was introduced. |

## Usage Guidelines

None

### Example

The following example shows you how to clear all rogue APs or rogue APs with specific MAC addresses:

```
Device# clear wireless wps rogue ap all
```

```
Device# clear wireless wps rogue ap mac-address 10.10.1
```

# clear wireless wps rogue client

To clear all rogue clients or client with specific MAC addresses, use the **clear wireless wps rogue client** command.

**clear wireless wps rogue client** { **all** | **mac-address** *<MAC Address>* }

## Syntax Description

|  |  |
|---|---|
| **all** | Clears all the rogue clients. |
| **mac-address** *<MAC Address>* | Clears the rogue clients with specific MAC addresses. |

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Amsterdam 16.12.1 | This command was introduced. |

## Usage Guidelines

None

### Example

The following example shows you how to clear all rogue clients or rogue clients with specific MAC addresses:

```
Device# clear wireless wps rogue client all
```

```
Device# clear wireless wps rogue client mac-address 10.10.1
```

# clear wireless wps rogue stats

To clear rogue statistics, use the **clear wireless wps rogue stats** command.

**clear wireless wps rogue stats**

### Syntax Description

This command has no arguments.

### Command Default

None

### Command Modes

Privileged EXEC (#)

### Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Amsterdam 16.12.1 | This command was introduced. |

### Usage Guidelines

None

### Example

The following example shows you how to clear rogue statistics:

```
Device# clear wireless wps rogue stats
```

# client-access (mesh)

To configure backhaul with client access AP for a mesh AP profile, use the **client-access** command.

**client-access**

## Syntax Description

This command has no keywords or arguments.

## Command Default

Backhaul client access is disabled.

## Command Modes

config-wireless-mesh-profile

## Command History

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

### Example

The following example shows how to configure backhaul with client access AP for a mesh AP profile:

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

# client association limit

To configure the maximum number of client connections on a WLAN, use the **client association limit** command. To disable clients association limit on the WLAN, use the **no** form of this command.

**client association limit** {*association-limit*}
**no client association limit** {*association-limit*}

## Syntax Description

| | |
|---|---|
| *association-limit* | Number of client connections to be accepted. The range is from 0 to . A value of zero (0) indicates no set limit. |

## Command Default

The maximum number of client connections is set to 0 (no limit).

## Command Modes

WLAN configuration

## Command History

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

## Usage Guidelines

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

This example shows how to configure a client association limit on a WLAN and configure the client limit to 200:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# shutdown
Device(config-wlan)# client association limit 200
Device(config-wlan)# no shutdown
Device(config-wlan)# end
```

This example shows how to disable a client association limit on a WLAN:

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

This example shows how to configure a client association limit per radio on a WLAN and configure the client limit to 200:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# client association limit radio 200
Device(config-wlan)# no shutdown
Device(config-wlan)# end
```

This example shows how to configure a client association limit per AP on a WLAN and configure the client limit to 300::

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# client association limit ap 300
Device(config-wlan)# no shutdown
Device(config-wlan)# end
```

# channel foreign

To configure the RF Profile DCA foreign AP contribution, use the **channel foreign** command. To disable the DCA Foreign AP Contribution, use the **no** form of this command.

**channel foreign**

## Syntax Description

| | |
|---|---|
| **foreign** | Configures the RF Profile DCA foreign AP contribution. |

## Command Default

None

## Command Modes

config-rf-profile

## Command History

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

## Usage Guidelines

None

This example shows how to configure the RF profile DCA foreign AP contribution.

```
Device(config-rf-profile)#channel foreign
```

# client-l2-vnid

To configure the client l2-vnid on a wireless fabric profile, use the **client-l2-vnid** command.

**client-l2-vnid** *vnid*

## Syntax Description

| | |
|---|---|
| *vnid* | Configures client l2-vnid. Valid range is 0 to 16777215. |

## Command Default

None

## Command Modes

config-wireless-fabric

## Command History

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

### Examples

The following example shows how to configure the client l2-vnid value on a wireless fabirc profile:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile fabric fabric-profile-name
Device(config-wireless-fabric)# client-l2-vnid 10
```

# collect counter

To configure the number of bytes or packets in a flow as a non-key field for a flow record, use the **collect counter** command in flow record configuration mode. To disable the use of the number of bytes or packets in a flow (counters) as a non-key field for a flow record, use the **no** form of this command.

## Command Default

The number of bytes or packets in a flow is not configured as a non-key field.

## Command Modes

Flow record configuration

## Command History

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

## Usage Guidelines

To return this command to its default settings, use the **no collect counter** or **default collect counter** flow record configuration command.

The following example configures the total number of bytes in the flows as a non-key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)#collect counter bytes long
```

The following example configures the total number of packets from the flows as a non-key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect counter packets long
```

# collect wireless ap mac address (wireless)

To enable the collection of MAC addresses of the access points that the wireless client is associated with, use the **collect wireless ap mac address** command in the flow record configuration mode. To disable the collection of access point MAC addresses, use the **no** form of this command.

**collect wireless ap mac address**
**no collect wirelessap mac address**

## Syntax Description

This command has no arguments or keywords.

## Command Default

The collection of access point MAC addresses is not enabled by default.

## Command Modes

Flow record configuration

## Command History

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

## Usage Guidelines

The Flexible NetFlow **collect** commands are used to configure non-key fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in non-key fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a non-key field does not create a new flow. In most cases, the values for non-key fields are taken from only the first packet in the flow.

The following example configures the flow record to enable the collection of MAC addresses of the access points that the wireless client is associated with:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect wireless ap mac address
```

# collect wireless client mac address (wireless)

To enable the collection of MAC addresses of the wireless clients that the access point is associated with, use the **collect wireless client mac address** command in the flow record configuration mode. To disable the collection of access point MAC addresses, use the **no** form of this command.

**collect wirelessclient mac address**
**no collect wireless client mac address**

## Syntax Description

This command has no arguments or keywords.

## Command Default

The collection of wireless client MAC addresses is not enabled by default.

## Command Modes

Flow record configuration

## Command History

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

## Usage Guidelines

The Flexible NetFlow **collect** commands are used to configure non-key fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in non-key fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a non-key field does not create a new flow. In most cases, the values for non-key fields are taken from only the first packet in the flow.

The following example configures the flow record to enable the collection of MAC addresses of the access points that the wireless client is associated with:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect wireless client mac address
```

# convergence

To configure mesh convergence method, use the **convergence** command.

**convergence** { **fast** | **noise-tolerant-fast** | **standard** | **very-fast** }

## Syntax Description

| | |
|---|---|
| **fast** | Configures fast convergence method. |
| **noise-tolerant-fast** | Configures noise-tolerant fast convergence method method to handle unstable RF environment. |
| **standard** | Configures standard convergence method. |
| **very-fast** | Configures very fast convergence method. |

## Command Default

Standard

## Command Modes

config-wireless-mesh-profile

## Command History

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

### Examples

The following example shows how to configure the fast convergence method for a mesh AP profile:

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

# coverage

To configure the voice and data coverage, use the **coverage** command. To reset the minimum RSSI value use the **no** form of this command.

**coverage** {**data** | **voice**} **rssi threshold** *value*

## Syntax Description

| | |
|---|---|
| **data** | Configure Coverage Hole Detection for data packets. |
| **voice** | Configure Coverage Hole Detection for voice packets. |
| *value* | Minimum RSSI value for the packets received by the access point. The valid rage is between –90 and –60 dBm. |

## Command Default

None

## Command Modes

config-rf-profile

## Command History

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

## Usage Guidelines

None

This example shows how to configure the coverage hole detection for data packets.

```
Device(config-rf-profile)#coverage data rssi threshold -85
```

# crypto key generate rsa

To generate Rivest, Shamir, and Adelman (RSA) key pairs, use the **crypto key generate rsa** commandinglobal configuration mode.

**crypto key generate rsa** [**general-keys** | **usage-keys** | **signature** | **encryption**] [**label** *key-label*] [**exportable**] [**modulus** *modulus-size*] [**storage** *devicename* **:**] [**redundancy**] [**on** *devicename* **:**]

## Syntax Description

| | |
|---|---|
| **general-keys** | (Optional) Specifies that a general-purpose key pair will be generated, which is the default. |
| **usage-keys** | (Optional) Specifies that two RSA special-usage key pairs, one encryption pair and one signature pair, will be generated. |
| **signature** | (Optional) Specifies that the RSA public key generated will be a signature special usage key. |
| **encryption** | (Optional) Specifies that the RSA public key generated will be an encryption special usage key. |
| **label** *key-label* | (Optional) Specifies the name that is used for an RSA key pair when they are being exported.<br>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.<br>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.<br>**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 (:).<br>Keys created on a USB token must be 2048 bits or less. |

## Command Default

RSA key pairs do not exist.

## Command Modes

Global configuration (config)

From Cisco IOS XE Release 17.11.1a, the command mode is Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 11.3 | This command was introduced. |
| 12.2(8)T | The *key-label* argumentwas added. |
| 12.2(15)T | The **exportable** keyword was added. |
| 12.2(18)SXD | This command was integrated into Cisco IOS Release 12.2(18)SXD. |
| 12.4(4)T | The **storage** keyword and *devicename* **:** argument were added. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.4(11)T | The **storage** keyword and *devicename* **:** argument were implemented on the Cisco 7200VXR NPE-G2 platform.<br>The **signature**, **encryption** and **on** keywords and *devicename* **:** argument were added. |
| 12.4(24)T | Support for IPv6 Secure Neighbor Discovery (SeND) was added. |
| XE 2.4 | The maximum RSA key size was expanded from 2048 to 4096 bits for private key operations. |
| 15.0(1)M | This command was modified. The **redundancy** keyword was introduced. |
| 15.1(1)T | This command was modified. The range value for the **modulus** keyword value is extended from 360 to 2048 bits to 360 to 4096 bits. |
| 15.2(2)SA2 | This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches. |
| Cisco IOS XE Release 17.11.1a | The default command mode for this command has changed from Global configuration (config) to Privileged EXEC (#). |

## Usage Guidelines

**Note** Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

Use this command to generate RSA key pairs for your Cisco device (such as a router).

RSA keys are generated in pairs--one public RSA key and one private RSA key.

If your router already has RSA keys when you issue this command, you will be warned and prompted to replace the existing keys with new keys.

**Note** Before issuing this command, ensure that your router has a hostname and IP domain name configured (with the **hostname** and **ip domain-name** commands). You will be unable to complete the **crypto key generate rsa** command without a hostname and IP domain name. (This situation is not true when you generate only a named key pair.)

**Note** Secure Shell (SSH) may generate an additional RSA key pair if you generate a key pair on a router having no RSA keys. The additional key pair is used only by SSH and will have a name such as {*router_FQDN* }.server. For example, if a router name is “router1.cisco.com,” the key name is “router1.cisco.com.server.”

This command is not saved in the router configuration; however, the RSA keys generated by this command are saved in the private configuration in NVRAM (which is never displayed to the user or backed up to another device) the next time the configuration is written to NVRAM.

**Note** If the configuration is not saved to NVRAM, the generated keys are lost on the next reload of the router.

There are two mutually exclusive types of RSA key pairs: special-usage keys and general-purpose keys. When you generate RSA key pairs, you will be prompted to select either special-usage keys or general-purpose keys.

### Special-Usage Keys

If you generate special-usage keys, two pairs of RSA keys will be generated. One pair will be used with any Internet Key Exchange (IKE) policy that specifies RSA signatures as the authentication method, and the other pair will be used with any IKE policy that specifies RSA encrypted keys as the authentication method.

A CA is used only with IKE policies specifying RSA signatures, not with IKE policies specifying RSA-encrypted nonces. (However, you could specify more than one IKE policy and have RSA signatures specified in one policy and RSA-encrypted nonces in another policy.)

If you plan to have both types of RSA authentication methods in your IKE policies, you may prefer to generate special-usage keys. With special-usage keys, each key is not unnecessarily exposed. (Without special-usage keys, one key is used for both authentication methods, increasing the exposure of that key.)

### General-Purpose Keys

If you generate general-purpose keys, only one pair of RSA keys will be generated. This pair will be used with IKE policies specifying either RSA signatures or RSA encrypted keys. Therefore, a general-purpose key pair might get used more frequently than a special-usage key pair.

### Named Key Pairs

If you generate a named key pair using the *key-label*argument, you must also specify the **usage-keys** keyword or the **general-keys** keyword. Named key pairs allow you to have multiple RSA key pairs, enabling the Cisco IOS software to maintain a different key pair for each identity certificate.

### Modulus Length

When you generate RSA keys, you will be prompted to enter a modulus length. The longer the modulus, the stronger the security. However a longer modules takes longer to generate (see the table below for sample times) and takes longer to use.

*Table 7: Sample Times by Modulus Length to Generate RSA Keys*

| Router | 360 bits | 512 bits | 1024 bits | 2048 bits (maximum) |
|---|---|---|---|---|
| Cisco 2500 | 11 seconds | 20 seconds | 4 minutes, 38 seconds | More than 1 hour |
| Cisco 4700 | Less than 1 second | 1 second | 4 seconds | 50 seconds |

Cisco IOS software does not support a modulus greater than 4096 bits. A length of less than 512 bits is normally not recommended. In certain situations, the shorter modulus may not function properly with IKE, so we recommend using a minimum modulus of 2048 bits.

**Note** As of Cisco IOS Release 12.4(11)T, peer *public* RSA key modulus values up to 4096 bits are automatically supported. The largest private RSA key modulus is 4096 bits. Therefore, the largest RSA private key a router may generate or import is 4096 bits. However, RFC 2409 restricts the private key size to 2048 bits or less for RSA encryption. The recommended modulus for a CA is 2048 bits; the recommended modulus for a client is 2048 bits.

Additional limitations may apply when RSA keys are generated by cryptographic hardware. For example, when RSA keys are generated by the Cisco VPN Services Port Adapter (VSPA), the RSA key modulus must be a minimum of 384 bits and must be a multiple of 64.

Specifying a Storage Location for RSA Keys

When you issue the **crypto key generate rsa** command with the **storage** *devicename* **:** keyword and argument, the RSA keys will be stored on the specified device. This location will supersede any **crypto key storage** command settings.

**Specifying a Device for RSA Key Generation**

As of Cisco IOS Release 12.4(11)T and later releases, you may specify the device where RSA keys are generated. Devices supported include NVRAM, local disks, and USB tokens. If your router has a USB token configured and available, the USB token can be used as cryptographic device in addition to a storage device. Using a USB token as a cryptographic device allows RSA operations such as key generation, signing, and authentication of credentials to be performed on the token. The private key never leaves the USB token and is not exportable. The public key is exportable.

RSA keys may be generated on a configured and available USB token, by the use of the **on** *devicename* **:** keyword and argument. Keys that reside on a USB token are saved to persistent token storage when they are generated. The number of keys that can be generated on a USB token is limited by the space available. If you attempt to generate keys on a USB token and it is full you will receive the following message:

```
% Error in generating keys:no available resources
```

Key deletion will remove the keys stored on the token from persistent storage immediately. (Keys that do not reside on a token are saved to or deleted from nontoken storage locations when the **copy**or similar command is issued.)

For information on configuring a USB token, see “ Storing PKI Credentials ” chapter in the Cisco IOS Security Configuration Guide, Release 12.4T. For information on using on-token RSA credentials, see the “ Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment ” chapter in the Cisco IOS Security Configuration Guide , Release 12.4T.

**Specifying RSA Key Redundancy Generation on a Device**

You can specify redundancy for existing keys only if they are exportable.

## Examples

The following example generates a general-usage 1024-bit RSA key pair on a USB token with the label “ms2” with crypto engine debugging messages shown:

```
Router(config)# crypto key generate rsa label ms2 modulus 2048 on usbtoken0:
The name for the keys will be: ms2
% The key modulus size is 2048 bits
% Generating 1024 bit RSA keys, keys will be on-token, non-exportable...
Jan 7 02:41:40.895: crypto_engine: Generate public/private keypair [OK]
Jan 7 02:44:09.623: crypto_engine: Create signature
Jan 7 02:44:10.467: crypto_engine: Verify signature
Jan 7 02:44:10.467: CryptoEngine0: CRYPTO_ISA_RSA_CREATE_PUBKEY(hw)(ipsec)
Jan 7 02:44:10.467: CryptoEngine0: CRYPTO_ISA_RSA_PUB_DECRYPT(hw)(ipsec)
```

Now, the on-token keys labeled “ms2” may be used for enrollment.

The following example generates special-usage RSA keys:

```
Router(config)# crypto key generate rsa usage-keys
The name for the keys will be: myrouter.example.com
Choose the size of the key modulus in the range of 360 to 2048 for your Signature Keys.
Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus[512]? <return>
Generating RSA keys.... [OK].
Choose the size of the key modulus in the range of 360 to 2048 for your Encryption Keys.
Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus[512]? <return>
Generating RSA keys.... [OK].
```

The following example generates general-purpose RSA keys:

**Note** You cannot generate both special-usage and general-purpose keys; you can generate only one or the other.

```
Router(config)# crypto key generate rsa general-keys
The name for the keys will be: myrouter.example.com
Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose
Keys. Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus[512]? <return>
Generating RSA keys.... [OK].
```

The following example generates the general-purpose RSA key pair “exampleCAkeys”:

```
crypto key generate rsa general-keys label exampleCAkeys
crypto ca trustpoint exampleCAkeys
 enroll url
http://exampleCAkeys/certsrv/mscep/mscep.dll
 rsakeypair exampleCAkeys 1024 1024
```

The following example specifies the RSA key storage location of “usbtoken0:” for “tokenkey1”:

crypto key generate rsa general-keys label tokenkey1 storage usbtoken0:

The following example specifies the **redundancy** keyword:

```
Router(config)# crypto key generate rsa label MYKEYS redundancy
```

The name for the keys will be: MYKEYS

Choose the size of the key modulus in the range of 360 to 2048 for your

General Purpose Keys. Choosing a key modulus greater than 512 may take

a few minutes.

How many bits in the modulus [512]:

% Generating 512 bit RSA keys, keys will be non-exportable with redundancy...[OK]

## Related Commands

| Command | Description |
|---|---|
| copy | Copies any file from a source to a destination, use the copy command in privileged EXEC mode. |
| **crypto key storage** | Sets the default storage location for RSA key pairs. |
| **debug crypto engine** | Displays debug messages about crypto engines. |
| **hostname** | Specifies or modifies the hostname for the network server. |
| **ip domain-name** | Defines a default domain name to complete unqualified hostnames (names without a dotted-decimal domain name). |
| **show crypto key mypubkey rsa** | Displays the RSA public keys of your router. |
| show crypto pki certificates | Displays information about your PKI certificate, certification authority, and any registration authority certificates. |

# cts inline-tagging

To configure Cisco TrustSec (CTS) inline tagging, use the **cts inline-tagging** command.

**cts inline-tagging**

## Syntax Description

This command has no keywords or arguments.

## Command Default

Inline tagging is not configured.

## Command Modes

wireless policy configuration (config-wireless-policy)

## Command History

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

### Example

This example shows how to configure CTS inline tagging.

```
Device(config-wireless-policy)# cts inline-tagging
```

# cts role-based enforcement

To configure Cisco TrustSec (CTS) SGACL enforcement, use the **cts role-based enforcement** command.

**cts role-based enforcement**

### Syntax Description

This command has no keywords or arguments.

### Command Default

SGACL is not enforced.

### Command Modes

wireless policy configuration (config-wireless-policy)

### Command History

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

### Example

This example shows how to configure CTS SGACL enforcement.

```
Device(config-wireless-policy)# cts role-based enforcement
```

# cts sgt

To set the Cisco TrustSec (CTS) default security group tag (SGT), use the **cts sgt** command.

**cts sgt** *sgt-value*

## Syntax Description

| | |
|---|---|
| *sgt-value* | Security group tag value. |

## Command Default

SGT tag is not set.

## Command Modes

wireless policy configuration (config-wireless-policy)

## Command History

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

### Example

This example shows how to set the default SGT.

```
Device(config-wireless-policy)# cts sgt 100
```

# custom-page login device

To configure a customized login page, use the **custom-page login device** command.

**custom-page login device** *html-filename*

## Syntax Description

| | |
|---|---|
| *html-filename* | Enter the HTML filename of the login page. |

## Command Default

None

## Command Modes

config-params-parameter-map

## Command History

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

### Examples

The following example shows how to configure a customized login page:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# parameter-map type webauth parameter-map-name
Device(config-params-parameter-map)# custom-page login device bootflash:login.html
```

# default

To set the parameters to their default values, use the **default** command.

**default** {**aaa-override** | **accounting-list** | **band-select** | **broadcast-ssid** | **call-snoop** | **ccx** | **channel-scan** | **parameters** | **chd** | **client** | **datalink** | **diag-channel** | **dtim** | **exclusionlist** | **ip** | **ipv6** | **load-balance** | **local-auth** | **mac-filtering** | **media-stream** | **mfp** | **mobility** | **nac** | **passive-client** | **peer-blocking** | **radio** | **roamed-voice-client** | **security** | **service-policy** | **session-timeout** | **shutdown** | **sip-cac** | **static-ip** | **uapsd** | **wgb** | **wmm**}

## Syntax Description

| | |
|---|---|
| **aaa-override** | Sets the AAA override parameter to its default value. |
| **accounting-list** | Sets the accounting parameter and its attributes to their default values. |
| **band-select** | Sets the band selection parameter to its default values. |
| **broadcast-ssid** | Sets the broadcast Service Set Identifier (SSID) parameter to its default value. |
| **call-snoop** | Sets the call snoop parameter to its default value. |
| **ccx** | Sets the Cisco client extension (Cisco Aironet IE) parameters and attributes to their default values. |
| **channel-scan** | Sets the channel scan parameters and attributes to their default values. |
| **chd** | Sets the coverage hold detection parameter to its default value. |
| **client** | Sets the client parameters and attributes to their default values. |
| **datalink** | Sets the datalink parameters and attributes to their default values. |
| **diag-channel** | Sets the diagnostic channel parameters and attributes to their default values. |
| **dtim** | Sets the Delivery Traffic Indicator Message (DTIM) parameter to its default value. |
| **exclusionlist** | Sets the client exclusion timeout parameter to its default value. |
| **ip** | Sets the IP parameters to their default values. |
| **ipv6** | Sets the IPv6 parameters and attributes to their default values. |
| **load-balance** | Sets the load-balancing parameter to its default value. |
| **local-auth** | Sets the Extensible Authentication Protocol (EAP) profile parameters and attributes to their default values. |
| **mac-filtering** | Sets the MAC filtering parameters and attributes to their default values. |
| **media-stream** | Sets the media stream parameters and attributes to their default values. |

| | |
|---|---|
| **mfp** | Sets the Management Frame Protection (MPF) parameters and attributes to their default values. |
| **mobility** | Sets the mobility parameters and attributes to their default values. |
| **nac** | Sets the RADIUS Network Admission Control (NAC) parameter to its default value. |
| **passive-client** | Sets the passive client parameter to its default value. |
| **peer-blocking** | Sets the peer to peer blocking parameters and attributes to their default values. |
| **radio** | Sets the radio policy parameters and attributes to their default values. |
| **roamed-voice-client** | Sets the roamed voice client parameters and attributes to their default values. |
| **security** | Sets the security policy parameters and attributes to their default values. |
| **service-policy** | Sets the WLAN quality of service (QoS) policy parameters and attributes to their default values. |
| **session-timeout** | Sets the client session timeout parameter to its default value. |
| **shutdown** | Sets the shutdown parameter to its default value. |
| **sip-cac** | Sets the Session Initiation Protocol (SIP) Call Admission Control (CAC) parameters and attributes to their default values. |
| **static-ip** | Sets the static IP client tunneling parameters and their attributes to their default values. |
| **uapsd** | Sets the Wi-Fi Multimedia (WMM) Unscheduled Automatic Power Save Delivery (UAPSD) parameters and attributes to their default values. |
| **wgb** | Sets the Workgroup Bridges (WGB) parameter to its default value. |
| **wmm** | Sets the WMM parameters and attributes to their default values. |

### Command Default

None.

### Command Modes

WLAN configuration

### Command History

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

### Usage Guidelines

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

This example shows how to set the Cisco Client Extension parameter to its default value:

```
Device(config-wlan)# default ccx aironet-iesupport
```

# debug platform qos-acl-tcam

To enable debugging of the quality of service (QoS) and access control list (ACL) hardware memory manager software, use the **debug platform qos-acl-tcam** command in privileged or user EXEC mode. To disable debugging, use the **no** form of this command.

**debug platform qos-acl-tcam** {**all** | **ctcam** | **errors** | **labels** | **mask** | **rpc** | **tcam**}
**no debug platform qos-acl-tcam** {**all** | **ctcam** | **errors** | **labels** | **mask** | **rpc** | **tcam**}

## Syntax Description

| | |
|---|---|
| **all** | Displays all QoS and ACL ternary content addressable memory (QATM) manager debug messages. |
| **ctcam** | Displays Cisco TCAM (CTCAM) related-events debug messages. |
| **errors** | Displays QATM error-related-events debug messages. |
| **labels** | Displays QATM label-related-events debug messages. |
| **mask** | Displays QATM mask-related-events debug messages. |
| **rpc** | Displays QATM remote procedure call (RPC) related-events debug messages. |
| **tcam** | Displays QATM hardware-memory-related events debug messages. |

## Command Default

Debugging is disabled.

## Command Modes

User EXEC

Privileged EXEC

## Command History

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

## Usage Guidelines

The **undebug platform qos-acl-tcam** command is the same as the **no debug platform qos-acl-tcam** command.

When you enable debugging on a switch stack, it is enabled only on the active switch. To enable debugging on a stack member, you can start a session from the active switch by using the **session** *switch-number* EXEC command. Then enter the **debug** command at the command-line prompt of the stack member. You also can use the **remote command** *stack-member-number LINE* EXEC command on the active switch to enable debugging on a member switch without first starting a session.

# debug qos-manager

To enable debugging of the quality of service (QoS) manager software, use the **debug qos-manager** command in privileged EXEC mode. Use the **no** form of this command to disable debugging.

**debug qos-manager** {**all** | **event** | **verbose**}
**no debug qos-manager** {**all** | **event** | **verbose**}

## Syntax Description

| | |
|---|---|
| **all** | Display all QoS-manager debug messages. |
| **event** | Display QoS-manager related-event debug messages. |
| **verbose** | Display QoS-manager detailed debug messages. |

## Command Default

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

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

## Usage Guidelines

The **undebug qos-manager** command is the same as the **no debug qos-manager** command.

# description

To configure a description for a flow monitor, flow exporter, or flow record, use the **description** command in the appropriate configuration mode. To remove a description, use the **no** form of this command.

**description** *description*
**no description** *description*

## Syntax Description

| | |
|---|---|
| *description* | Text string that describes the flow monitor, flow exporter, or flow record. |

## Command Default

The default description for a flow sampler, flow monitor, flow exporter, or flow record is "User defined."

## Command Modes

The following command modes are supported:

Flow exporter configuration

Flow monitor configuration

Flow record configuration

## Command History

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

## Usage Guidelines

To return this command to its default setting, use the **no description** or **default description** command in the appropriate configuration mode.

The following example configures a description for a flow monitor:

```
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)# description Monitors traffic to 172.16.0.1 255.255.0.0
```

# destination

To configure an export destination for a flow exporter, use the **destination** command in flow exporter configuration mode. To remove an export destination for a flow exporter, use the **no** form of this command.

**destination** {*hostnameip-address*}
**no destination** {*hostnameip-address*}

## Syntax Description

| | |
|---|---|
| *hostname* | Hostname of the device to which you want to send the NetFlow information. |
| *ip-address* | IPv4 address of the workstation to which you want to send the NetFlow information. |

## Command Default

An export destination is not configured.

## Command Modes

Flow exporter configuration

## Command History

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

## Usage Guidelines

Each flow exporter can have only one destination address or hostname.

When you configure a hostname instead of the IP address for the device, the hostname is resolved immediately and the IPv4 address is stored in the running configuration. If the hostname-to-IP-address mapping that was used for the original Domain Name System (DNS) name resolution changes dynamically on the DNS server, the device does not detect this, and the exported data continues to be sent to the original IP address, resulting in a loss of data.

To return this command to its default setting, use the **no destination** or **default destination** command in flow exporter configuration mode.

The following example shows how to configure the networking device to export the cache entry to a destination system:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# destination 10.0.0.4
```

# device-role (IPv6 snooping)

To specify the role of the device attached to the port, use the **device-role** command in IPv6 snooping configuration mode.

**device-role** {**node** | **switch**}

## Syntax Description

| | |
|---|---|
| **node** | Sets the role of the attached device to node. |
| **switch** | Sets the role of the attached device to switch. |

## Command Default

The device role is node.

## Command Modes

IPv6 snooping configuration

## Command History

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

## Usage Guidelines

The **device-role** command specifies the role of the device attached to the port. By default, the device role is node.

The **switch** keyword indicates that the remote device is a switch and that the local switch is now operating in multiswitch mode; binding entries learned from the port will be marked with trunk_port preference level. If the port is configured as a trust-port, binding entries will be marked with trunk_trusted_port preference level.

This example shows how to define an IPv6 snooping policy name as policy1, place the device in IPv6 snooping configuration mode, and configure the device as the node:

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# device-role node
```

# device-role (IPv6 nd inspection)

To specify the role of the device attached to the port, use the **device-role** command in neighbor discovery (ND) inspection policy configuration mode.

**device-role** {**host** | **monitor** | **router** | **switch**}

## Syntax Description

| | |
|---|---|
| **host** | Sets the role of the attached device to host. |
| **monitor** | Sets the role of the attached device to monitor. |
| **router** | Sets the role of the attached device to router. |
| **switch** | Sets the role of the attached device to switch. |

## Command Default

The device role is host.

## Command Modes

ND inspection policy configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |
| | The keywords **monitor** and **router** are deprecated. |

## Usage Guidelines

The **device-role** command specifies the role of the device attached to the port. By default, the device role is host, and therefore all the inbound router advertisement and redirect messages are blocked. If the device role is enabled using the **router** keyword, all messages (router solicitation [RS], router advertisement [RA], or redirect) are allowed on this port.

When the **router** or **monitor** keyword is used, the multicast RS messages are bridged on the port, regardless of whether limited broadcast is enabled. However, the monitor keyword does not allow inbound RA or redirect messages. When the monitor keyword is used, devices that need these messages will receive them.

The **switch** keyword indicates that the remote device is a switch and that the local switch is now operating in multiswitch mode; binding entries learned from the port will be marked with trunk_port preference level. If the port is configured as a trust-port, binding entries will be marked with trunk_trusted_port preference level.

The following example defines a Neighbor Discovery Protocol (NDP) policy name as policy1, places the device in ND inspection policy configuration mode, and configures the device as the host:

```
Device(config)#  ipv6 nd inspection policy policy1
Device(config-nd-inspection)# device-role host
```

# device-tracking binding vlan

To configure IPv4 or IPv6 static entry, use the **device-tracking binding vlan** command.

**device-tracking binding vlan** *vlan-id* {*ipv4-addr ipv6-addr* }**interface gigabitEthernet** *ge-intf-num hardware-or-mac-address*

## Syntax Description

| | |
|---|---|
| *vlan-id* | VLAN ID. Valid range is 1 to 4096. |
| *ipv4-addr* | IPv4 address of the device. |
| *ipv6-addr* | IPv6 address of the device. |
| **interface gigabitEthernet** | GigabitEthernet IEEE 802.3z. |
| *ge-intf-num* | GigabitEthernet interface number. Valid range is 1 to 32. |
| *hardware-or-mac-address* | The 48-bit hardware address or the MAC address of the device. |

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

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

### Examples

The following example shows how to configure IPv4 static entry:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# device-tracking binding vlan 20 20.20.20.5 interface gigabitEthernet 1
0000.1111.2222
```

# device-tracking policy

To configure a Switch Integrated Security Features (SISF)-based IP device tracking policy, use the **device-tracking** command in global configuration mode. To delete a device tracking policy, use the **no** form of this command.

**device -tracking policy** *policy-name*
**no device-tracking policy** *policy-name*

## Syntax Description

| | |
|---|---|
| *policy-name* | User-defined name of the device tracking policy. The policy name can be a symbolic string (such as Engineering) or an integer (such as 0). |

## Command Default

A device tracking policy is not configured.

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines

Use the SISF-based **device-tracking policy** command to create a device tracking policy. When the **device-tracking policy** command is enabled, the configuration mode changes to device-tracking configuration mode. In this mode, the administrator can configure the following first-hop security commands:

- (Optional) **device-role**{**node**] | **switch**}—Specifies the role of the device attached to the port. Default is **node**.
- (Optional) **limit address-count** *value*—Limits the number of addresses allowed per target.
- (Optional) **no**—Negates a command or sets it to defaults.
- (Optional) **destination-glean**{**recovery**| **log-only**}[**dhcp**]}—Enables binding table recovery by data traffic source address gleaning.
- (Optional) **data-glean**{**recovery**| **log-only**}[**dhcp** | **ndp**]}—Enables binding table recovery using source or data address gleaning.
- (Optional) **security-level**{**glean**|**guard**|**inspect**}—Specifies the level of security enforced by the feature. Default is **guard.**

  **glean**—Gleans addresses from messages and populates the binding table without any verification.
  **guard**—Gleans addresses and inspects messages. In addition, it rejects RA and DHCP server messages. This is the default option.
  **inspect**—Gleans addresses, validates messages for consistency and conformance, and enforces address ownership.
- (Optional) **tracking** {**disable** | **enable**}—Specifies a tracking option.
- (Optional) **trusted-port**—Sets up a trusted port. It disables the guard on applicable targets. Bindings learned through a trusted port have preference over bindings learned through any other port. A trusted port is given preference in case of a collision while making an entry in the table.

This example shows how to configure an a device-tracking policy:

```
Device(config)# device-tracking policy policy1
Device(config-device-tracking)# trusted-port
```

# dhcp-tlv-caching

To configure DHCP TLV caching on a WLAN, use the **dhcp-tlv-caching** command.

**dhcp-tlv-caching**

## Command Default

None

## Command Modes

config-wireless-policy

## Command History

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

### Example

This example shows how to configure DHCP TLV caching on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy rr-xyz-policy-1
Device(config-wireless-policy)# dhcp-tlv-caching
Device(config-wireless-policy)# radius-profiling
Device(config-wireless-policy)# end
```

# dns-server (IPv6)

To specify the Domain Name System (DNS) IPv6 servers available to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **dns-server** command in DHCP for IPv6 pool configuration mode. To remove the DNS server list, use the **no** form of this command.

**dns-server** *ipv6-address*
**no dns-server** *ipv6-address*

## Syntax Description

| | |
|---|---|
| *ipv6-address* | The IPv6 address of a DNS server.<br>This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. |

## Command Default

When a DHCP for IPv6 pool is first created, no DNS IPv6 servers are configured.

## Command Modes

DHCP for IPv6 pool configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(4)T | This command was introduced. |
| Cisco IOS XE Release 2.1 | This command was integrated into Cisco IOS XE Release 2.1. |
| 12.2(33)SRE | This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE. |

| | |
|---|---|
| 12.2(33)XNE | This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE. |

## Usage Guidelines

Multiple Domain Name System (DNS) server addresses can be configured by issuing this command multiple times. New addresses will not overwrite old addresses.

## Examples

The following example specifies the DNS IPv6 servers available:

```
dns-server 2001:0DB8:3000:3000::42
```

## Related Commands

| Command | Description |
|---|---|
| **domain-name** | Configures a domain name for a DHCP for IPv6 client. |
| **ipv6 dhcp pool** | Configures a DHCP for IPv6 configuration information pool and enters DHCP for IPv6 pool configuration mode. |

# dnscrypt

To enable or disable DNScrypt, use the **dnscrypt** command.

**dnscrypt**

## Command Default

None

## Command Modes

config-profile

## Command History

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

## Usage Guidelines

By default, the DNScrypt option is enabled.

This example shows how to enable or disable DNScrypt:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# parameter-map type umbrella global
Device(config-profile)# token 57CC80106C087FB1B2A7BAB4F2F4373C00247166
Device(config-profile)# local-domain dns_wl
Device(config-profile)# no dnscrypt
Device(config-profile)# end
```

# domain-name (DHCP)

To specify the domain n ame for a Dynamic Host Configuration Protocol (DHCP) client, use the **domain-name** command in DHCP pool configuration mode. To remove the domain name, use the no form of this command.

**domain-name** *domain*
**no domain-name**

## Syntax Description

| | |
|---|---|
| *domain* | Specifies the domain name string of the client. |

## Command Default

No default behavior or values.

## Command Modes

DHCP pool configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(1)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Examples

The following example specifies cisco.com as the domain name of the client:

```
domain-name cisco.com
```

## Related Commands

| Command | Description |
|---|---|
| **dns-server** | Specifies the DNS IP servers available to a DHCP client. |
| **ip dhcp pool** | Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode. |

# dot11 airtime-fairness

To configure airtime-fairness policy for 2.4- or 5-GHz radio, use the **dot11 airtime-fairness** command.

**dot11** {**24ghz** | **5ghz** }**airtime-fairness** *atf-policy-name*

## Syntax Description

| | |
|---|---|
| *atf-policy-name* | Is the name of the airtime-fairness policy. |

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

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

This example shows how to configure airtime-fairness policy for 2.4- or 5-GHz radio:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy <profile-name>
Device(config-wireless-policy)# dot11 24ghz airtime-fairness <atf-policy-name>
Device(config-wireless-policy)# end
```

# dot11ax twt-broadcast-support

To configure TWT broadcast support on WLAN, use the **dot11ax twt-broadcast-support** command. To disable the feature, use the **no** command of the command.

**dot11ax twt-broadcast-support**

**[no] dot11ax twt-broadcast-support**

## Syntax Description

| | |
|---|---|
| **dot11ax twt-broadcast-support** | Configures the TWT broadcast support on WLAN |

## Command Default

None

## Command Modes

WLAN configuration

## Command History

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

### Example

This example shows how to configure target wakeup time on WLAN:

```
Device(config-wlan)# dot11ax twt-broadcast-support
```

# dot11 5ghz reporting-interval

To configure the client report interval sent from AP for clients on 802.11a radio, use the **dot11 5ghz reporting-interval** command.

**dot11 5ghz reporting-interval** *reporting-interval*

## Syntax Description

| | |
|---|---|
| *reporting-interval* | Interval at which client report needs to be sent in seconds. |

## Command Default

None

## Command Modes

config-ap-profile

## Command History

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

### Examples

The following example shows how to set the client report interval in seconds:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap profile profile-name
Device(config-ap-profile)# dot11 5ghz reporting-interval 8
```

# dot11 reporting-interval

To set the volume metering interval, use the **dot11 reporting-interval** command.

**dot11** {**24ghz** | **5ghz** } *reporting-interval*

## Syntax Description

| | |
|---|---|
| *reporting-interval* | Interval to send client accounting statistics. |

## Command Default

Interval is configured at the default level of 90 seconds.

## Command Modes

config-ap-profile

## Command History

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

## Usage Guidelines

Though the CLI allows you to configure range from 5 to 90 seconds, we recommend that you use 60 to 90 seconds range for Volume Metering.

This CLI can also be used to configure the interval when smart roam is enabled, which has a range of 5 to 90 seconds.

Though you can set two different values for volume metering and smart roam, only one value takes effect based on the order of execution. So, we recommend that you use the same reporting interval for both.

### Example

The following example shows how to configure volume metering:

```
Device(config-ap-profile)# dot11 24ghz 60
```

# dot1x system-auth-control

To globally enable 802.1X SystemAuthControl (port-based authentication), use the **dot1x system-auth-control**command in global configuration mode. To disable SystemAuthControl, use the **no** form of this command.

**dot1x system-auth-control**
**no dot1x system-auth-control**

### Syntax Description

This command has no arguments or keywords.

### Command Default

System authentication is disabled by default. If this command is disabled, all ports behave as if they are force authorized.

### Command Modes

Global configuration (config)

### Command History

| Release | Modification |
|---|---|
| 12.3(2)XA | This command was introduced. |
| 12.2(14)SX | This command was implemented on the Supervisor Engine 720. |
| 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T. |
| 12.2(17d)SXB | Support for this command on the Supervisor Engine 2 was extended to 12.2(17d)SXB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |

### Usage Guidelines

The IEEE 802.1x standard defines a client-server-based access control and authentication protocol that restricts unauthorized devices from connecting to a LAN through publicly accessible ports. 802.1x controls network access by creating two distinct virtual access points at each port. One access point is an uncontrolled port; the other is a controlled port. All traffic through the single port is available to both access points. 802.1x authenticates each user device that is connected to a switch port and assigns the port to a VLAN before making available any services that are offered by the switch or the LAN. Until the device is authenticated, 802.1x access control allows only Extensible Authentication Protocol (EAP) over LAN (EAPOL) traffic through the port to which the device is connected. After authentication is successful, normal traffic can pass through the port.

The **no** form of the command removes any 802.1X-related configurations.

You must enable Authentication, Authorization, and Accounting (AAA) and specify the authentication method list before enabling 802.1X. A method list describes the sequence and authentication methods to be queried to authenticate a user.

### Examples

The following example shows how to enable SystemAuthControl:

```
Router(config)# dot1x system-auth-control
```

## Related Commands

| Command | Description |
|---|---|
| **aaa authentication dot1x** | Specifies one or more AAA methods for use on interfaces running IEEE 802.1X. |
| **aaa new-model** | Enables the AAA access-control model. |
| **debug dot1x** | Displays 802.1X debugging information. |
| **description** | Specifies a description for an 802.1X profile. |
| **device** | Statically authorizes or rejects individual devices. |
| **dot1x initialize** | Initializes 802.1X state machines on all 802.1X-enabled interfaces. |
| **dot1x max-req** | Sets the maximum number of times that a router or Ethernet switch network module can send an EAP request/identity frame to a client (assuming that a response is not received) before restarting the authentication process. |
| **dot1x port-control** | Enables manual control of the authorized state of a controlled port. |
| **dot1x re-authenticate** | Manually initiates a reauthentication of the specified 802.1X-enabled ports. |
| **dot1x reauthentication** | Globally enables periodic reauthentication of the client PCs on the 802.1X interface. |
| **dot1x timeout** | Sets retry timeouts. |
| **identity profile** | Creates an identity profile and enters identity profile configuration mode. |
| **show dot1x** | Displays details and statistics for an identity profile. |
| **template** | Specifies a virtual template from which commands may be cloned. |

# eap profile

To configure an EAP profile, use the **eap profile** command.

**eap profile** *profile-name*

## Syntax Description

| | |
|---|---|
| *profile-name* | Name of the EAP profile. Maximum number of allowed characters is 63. |

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

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

### Examples

The following example shows how to configure an EAP profile name:

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

# et-analytics

To enable Encrypted Traffic Analytics (ETA) globally on Cisco Elastic Wireless LAN Controller (eWLC), use the **et-analytics** command.

**et-analytics**

## Command Default

None

## Command Modes

ET-Analytics configuration

## Command History

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

This example shows how to enable Encrypted Traffic Analytics (ETA) globally on Cisco Elastic Wireless LAN Controller (eWLC) in the ET-Analytics configuration mode:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# et-analytics
Device(config-et-analytics)# end
```

# ethernet-vlan-transparent (mesh)

To configure ethernet bridging VLAN transparency for a mesh AP profile, use the **ethernet-vlan-transparent** command.

**ethernet-vlan-transparent**

### Syntax Description

This command has no keywords or arguments.

### Command Default

Ethernet bridging VLAN transparency is enabled.

### Command Modes

config-wireless-mesh-profile

### Command History

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

## Example

The following example shows how to configure ethernet bridging VLAN transparency for a mesh AP profile:

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

# ethernet-bridging (mesh)

To configure ethernet bridging for a mesh AP profile, use the **ethernet-bridging** command.

**ethernet-bridging**

## Syntax Description

This command has no keywords or arguments.

## Command Default

Ethernet bridging is disabled.

## Command Modes

config-wireless-mesh-profile

## Command History

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

### Example

The following example shows how to configure ethernet bridging for a mesh AP profile:

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

# event identity-update

To specify the match criteria to a policy map, use the **event identity-update** command.

**event identity-update**[**match-all** | **match-first**]

## Syntax Description

| | |
|---|---|
| **match-all** | Evaluates all the classes. |
| **match-first** | Evaluates the first class. |

## Command Default

None

## Command Modes

config-event-control-policymap

## Command History

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

### Examples

The following example shows how to specify the match criteria as match all classes to a policy map:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# policy-map type control subscriber policy-map-name
Device(config-event-control-policymap)# event identity-update match-all
```

# exclusionlist

To configure an exclusion list, use the **exclusionlist** command. To disable an exclusion list, use the **no** form of this command.

**exclusionlist** [ **timeout** *seconds* ]
**no** **exclusionlist** [**timeout**]

## Syntax Description

| | |
|---|---|
| **timeout** *seconds* | (Optional) Specifies an exclusion list timeout in seconds. The range is from 0 to 2147483647. A value of zero (0) specifies no timeout. |

## Command Default

The exclusion list is set to 60 seconds.

## Command Modes

Wireless policy configuration

## Command History

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

This example shows how to configure a client exclusion list:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy default-policy-profile
Device(config-wireless-policy)# exclusionlist timeout 5
```

# exec-character-bits

To configure the character widths of EXEC and configuration command characters, use the **exec-character-bits** command in line configuration mode. To restore the default value, use the **no** form of this command.

**exec-character-bits** { *7* | *8* }

**no exec-character-bits**

## Syntax Description

| | |
|---|---|
| *7* | Sets the 7-bit character set. This is the default. |
| *8* | Sets the full 8-bit character set for use of international and graphical characters in banner messages, prompts, and so on. |

## Command Default

7-bit ASCII character set.

## Command Modes

Line configuration

## Command History

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

## Usage Guidelines

Setting the EXEC character width to 8 allows you to use special graphical and international characters in banners, prompts, and so on. However, setting the EXEC character width to 8 bits can cause failures. For example, if a user on a terminal that is sending parity enters the **help** command, an "unrecognized command" message appears because the system is reading all 8 bits, and the eighth bit is not needed for the **help** command.

## Examples

The following example shows how to configure the character widths of EXEC and configuration command characters :

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# line console 0
Device(config-line)# exec-character-bit 8
```

# exec time-out

To set the interval that the EXEC command interpreter waits until user input is detected, use the **exec-timeout** command in line configuration mode. To remove the timeout duration, use the **no** form of this command.

**exec time-out** *minutes* [ *seconds* ]

**exec time-out**

## Syntax Description

| | |
|---|---|
| *minutes* | Integer that specifies the number of minutes. The default is 10 minutes. |
| *seconds* | (Optional) Additional time intervals, in seconds. |

## Command Default

10 minutes

## Command Modes

Line configuration

## Command History

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

## Usage Guidelines

If no input is detected during the interval, the EXEC facility resumes the current connection. If no connections exist, the EXEC facility returns the terminal to the idle state and disconnects the incoming session.

To specify no timeout, enter the **exec-timeout 0 0** command.

## Examples

The following example sets a time interval of 2 minutes, 30 seconds:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# line console 0
Device(config-line)# exec-timeout 12 0
```

# exporter default-flow-exporter

To add an exporter to use to export records, use the **exporter default-flow-exporter** command. Use the **no** form of this command to disable the feature.

**exporter default-flow-exporter**

**[no] exporter default-flow-exporter**

## Syntax Description

There are no arguments to this command.

## Command Default

None

## Command Modes

Flow monitor configuration

## Command History

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

### Example

This example shows how to add an exporter to use to export records:

```
Device(config-flow-monitor)#exporter default-flow-exporter
```

# fabric control-plane

To configure the fabric control plane details, use the **fabric control-plane** command.

**fabric control-plane** *map-server-name*

## Syntax Description

| | |
|---|---|
| *map-server-name* | Refers to the fabric control plane name associated with the site tag. |

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

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

This example shows how to configure the fabric control plane details:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless tag site default-site-tag
Device(config-site-tag)# fabric control-plane
map-server-name
Device(config-site-tag)# end
```

# fallback-radio-shut

To configure shutdown of the radio interface, use the **fallback-radio-shut** command.

**fallback-radio-shut**

## Command Default

None

## Command Modes

config-wireless-flex-profile

## Command History

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

### Examples

The following example shows how to configure shutdown of the radio interface:

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

# flex

To configure flex related parameters, use the **flex** command.

**flex** {**nat-pat** | **split-mac-acl** *split-mac-acl-name* | **vlan-central-switching** }

## Syntax Description

| | |
|---|---|
| **nat-pat** | Enables NAT-PAT. |
| **split-mac-acl** | Configures split-mac-acl name. |
| *split-mac-acl-name* | Name of split MAC ACL. |
| **vlan-central-switching** | VLAN based central switching. |

## Command Default

None

## Command Modes

config-wireless-policy

## Command History

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

### Examples

The following example shows how to configure flex related VLAN central-switching:

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

# flow exporter

To create a flow exporter, or to modify an existing flow exporter, and enter flow exporter configuration mode, use the **flow exporter** command in global configuration mode. To remove a flow exporter, use the **no** form of this command.

**flow exporter** *exporter-name*
**no flow exporter** *exporter-name*

## Syntax Description

| | |
|---|---|
| *exporter-name* | Name of the flow exporter that is being created or modified. |

## Command Default

flow exporters are not present in the configuration.

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines

Flow exporters export the data in the flow monitor cache to a remote system, such as a server running NetFlow collector, for analysis and storage. Flow exporters are created as separate entities in the configuration. Flow exporters are assigned to flow monitors to provide data export capability for the flow monitors. You can create several flow exporters and assign them to one or more flow monitors to provide several export destinations. You can create one flow exporter and apply it to several flow monitors.

## Examples

The following example creates a flow exporter named FLOW-EXPORTER-1 and enters flow exporter configuration mode:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)#
```

# flow monitor

To create a flow monitor, or to modify an existing flow monitor, and enter flow monitor configuration mode, use the **flow monitor** command in global configuration mode. To remove a flow monitor, use the **no** form of this command.

**flow monitor** *monitor-name*
**no flow monitor** *monitor-name*

## Syntax Description

| | |
|---|---|
| *monitor-name* | Name of the flow monitor that is being created or modified. |

## Command Default

flow monitors are not present in the configuration.

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines

Flow monitors are the  component that is applied to interfaces to perform network traffic monitoring. Flow monitors consist of a flow record and a cache. You add the record to the flow monitor after you create the flow monitor. The flow monitor cache is automatically created at the time the flow monitor is applied to the first interface. Flow data is collected from the network traffic during the monitoring process based on the key and nonkey fields in the flow monitor's record and stored in the flow monitor cache.

## Examples

The following example creates a flow monitor named FLOW-MONITOR-1 and enters flow monitor configuration mode:

```
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)#
```

# flow record

To create a  flow record, or to modify an existing  flow record, and enter  flow record configuration mode, use the **flow record** command in global configuration mode. To remove a  record, use the **no** form of this command.

**flow record** *record-name*
**no flow record** *record-name*

## Syntax Description

| | |
|---|---|
| *record-name* | Name of the flow record that is being created or modified. |

## Command Default

A  flow record is not configured.

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines

A flow record defines the keys that  uses to identify packets in the flow, as well as other fields of interest that gathers for the flow. You can define a flow record with any combination of keys and fields of interest. The supports a rich set of keys. A flow record also defines the types of counters gathered per flow. You can configure 64-bit packet or byte counters.

## Examples

The following example creates a flow record named FLOW-RECORD-1, and enters  flow record configuration mode:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)#
```

# full-sector-dfs (mesh)

To configure mesh full sector Dynamic Frequency Selection (DFS) status for a mesh AP profile, use the **full-sector-dfs** command.

**full-sector-dfs**

## Syntax Description

This command has no keywords or arguments.

## Command Default

Full sector DFS is enabled.

## Command Modes

config-wireless-mesh-profile

## Command History

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

### Example

The following example shows how to configure mesh full sector DFS status for a mesh AP profile:

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

# Configuration Commands: g to z

# 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.<br>**Note** Ensure that the Hyperlocation threshold reset value is less than the threshold trigger value. |

## Command Modes

WLAN AP Group configuration

## Command History

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

- 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

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

### 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 CNTL/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.

**inactive-timeout** *timeout-in-seconds*

## Syntax Description

| | |
|---|---|
| *timeout-in-seconds* | Specifies the inactive flow timeout value. The range is from 1 to 604800. |

## Command Default

None

## Command Modes

ET-Analytics configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to enable in-active timer in the ET-Analytics configuration mode:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# et-analytics
Device(config-et-analytics)# inactive-timeout 15
Device(config-et-analytics)# end
```

# install activate

To activate an installed package, use the **install activate** command.

**install activate** {**auto-abort-timer** | **file** | **profile** | **prompt-level**}

## Syntax Description

| | |
|---|---|
| **auto-abort-timer** | Sets the cancel timer. The time range is between 30 and 1200 minutes. |
| **file** | Specifies the package to be activated. |
| **profile** | Specifies the profile to be activated. |
| **prompt-level** | Sets the prompt level. |

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.12.2s | This command was introduced. |

### Example

The following example shows how to activate the installed package:

```
Device# install activate profile default
install_activate: START Thu Nov 24 20:14:53 UTC 2019

System configuration has been modified.
Press Yes(y) to save the configuration and proceed.
Press No(n) for proceeding without saving the configuration.
Press Quit(q) to exit, you may save configuration and re-enter the command. [y/n/q] y
Building configuration...
[OK]Modified configuration has been saved
Jan 24 20:15:02.745: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
activate
Jan 24 20:15:02.745 %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
activate
install_activate: Activating PACKAGE
```

# install activate profile

To activate an installed package, use the **install activate profile** command.

**install activate profile**

### Syntax Description

| | |
|---|---|
| **profile** | To activate the profile. |

### Command Default

None

### Command Modes

Privileged EXEC (#)

### Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.12.2s | This command was introduced. |

### Example

The following example shows how to activate the installed package:

```
Device#install activate profile default
install_activate: START Thu Nov 24 20:14:53 UTC 2019

System configuration has been modified.
Press Yes(y) to save the configuration and proceed.
Press No(n) for proceeding without saving the configuration.
Press Quit(q) to exit, you may save configuration and re-enter the command. [y/n/q] y
Building configuration...
[OK]Modified configuration has been saved
Jan 24 20:15:02.745: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
activate
Jan 24 20:15:02.745 %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
activate
install_activate: Activating PACKAGE
```

# install remove profile default

To specify an install package that is to be removed, use the **install remove profile default** command.

**install remove profile default**

## Syntax Description

| | |
|---|---|
| **remove** | Removes the install package. |
| **profile** | Specifies the profile to be removed. |

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.11.1 | This command was introduced. |

### Example

The following example shows how to remove a default profile:

```
Device# install remove profile default
```

# install deactivate

To specify an install package that is to be deactivated, use the **install deactivate file** command.

**install deactivate file** *file-name*

## Syntax Description

|  |  |
|---|---|
| *file-name* | Specifies the package name. Options are: bootflash:, flash:, and webui:. |

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.11.1 | This command was introduced. |

### Example

The following example shows how to deactivate an install package:

```
Device# install deactivate file vwlc_apsp_16.11.1.0_74.bin
```

# install rollback

To roll back to a particular installation point, use the **install rollback** command.

**install rollback to** {**base** | **committed** | **id** *id* | **label** *label*} [**prompt-level none**]

## Syntax Description

| | |
|---|---|
| **base** | Rolls back to the base image. |
| **prompt-level none** | Sets the prompt level as none. |
| **committed** | Rolls back to the last committed installation point. |
| **id** | Rolls back to a specific install point ID. |
| **label** | Rolls back to a specific install point label. |

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.11.1 | This command was introduced. |

### Example

The following example shows how to specify the ID of the install point to roll back to:

```
Device# install rollback to id 1
```

# interface vlan

To create or access a dynamic switch virtual interface (SVI) and to enter interface configuration mode, use the **interface vlan** command in global configuration mode. To delete an SVI, use the **no** form of this command.

**interface vlan** *vlan-id*
**no interface vlan** *vlan-id*

## Syntax Description

| | |
|---|---|
| *vlan-id* | VLAN number. The range is 1 to 4094. |

## Command Default

The default VLAN interface is VLAN 1.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

SVIs are created the first time you enter the **interface vlan** *vlan-id* command for a particular VLAN. The *vlan-id* corresponds to the VLAN-tag associated with data frames on an IEEE 802.1Q encapsulated trunk or the VLAN ID configured for an access port.

**Note** When you create an SVI, it does not become active until it is associated with a physical port.

If you delete an SVI using the **no interface vlan** *vlan-id* command, it is no longer visible in the output from the **show interfaces** privileged EXEC command.

**Note** You cannot delete the VLAN 1 interface.

You can reinstate a deleted SVI by entering the **interface vlan** *vlan-id* command for the deleted interface. The interface comes back up, but the previous configuration is gone.

The interrelationship between the number of SVIs configured on a chassis or a chassis stack and the number of other features being configured might have an impact on CPU utilization due to hardware limitations. You can use the **sdm prefer** global configuration command to reallocate system hardware resources based on templates and feature tables.

You can verify your setting by entering the **show interfaces** and **show interfaces vlan** *vlan-id* privileged EXEC commands.

This example shows how to create a new SVI with VLAN ID 23 and enter interface configuration mode:

```
Device(config)# interface vlan 23
Device(config-if)#
```

# ip access-group

To configure WLAN access control group (ACL), use the **ip access-group** command. To remove a WLAN ACL group, use the **no** form of the command.

**ip access-group** [**web**] *acl-name*
**no ip access-group** [**web**]

## Syntax Description

| | |
|---|---|
| **web** | (Optional) Configures the IPv4 web ACL. |
| *acl-name* | Specify the preauth ACL used for the WLAN with the security type value as webauth. |

## Command Default

None

## Command Modes

WLAN configuration

## Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to configure a WLAN ACL:

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#wlan wlan1
Device(config-wlan)#ip access-group test-acl
```

This example shows how to configure an IPv4 WLAN web ACL:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# ip access-group web test
Device(config-wlan)#
```

# ip access-list extended

To configure extended access list, use the **ip access-list extended** command.

**ip access-list extended** {**<100-199>** | **<2000-2699>** *access-list-name*}

## Syntax Description

| | |
|---|---|
| **<100-199>** | Extended IP access-list number. |
| **<2000-2699>** | Extended IP access-list number (expanded range). |

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to configure extended access list:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ip access-list extended access-list-name
```

# ip address

To set a primary or secondary IP address for an interface, use the **ip address** command in interface configuration mode. To remove an IP address or disable IP processing, use the noform of this command.

**ip address** *ip-address mask* [**secondary** [**vrf** *vrf-name*]]
**no ip address** *ip-address mask* [**secondary** [**vrf** *vrf-name*]]

## Syntax Description

| | |
|---|---|
| *ip-address* | IP address. |
| *mask* | Mask for the associated IP subnet. |
| **secondary** | (Optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.<br>**Note** If the secondary address is used for a VRF table configuration with the **vrf** keyword, the **vrf** keyword must be specified also. |
| **vrf** | (Optional) Name of the VRF table. The *vrf-name* argument specifies the VRF name of the ingress interface. |

## Command Default

No IP address is defined for the interface.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

An interface can have one primary IP address and multiple secondary IP addresses. Packets generated by the Cisco IOS software always use the primary IP address. Therefore, all devices and access servers on a segment should share the same primary network number.

Hosts can determine subnet masks using the Internet Control Message Protocol (ICMP) mask request message. Devices respond to this request with an ICMP mask reply message.

You can disable IP processing on a particular interface by removing its IP address with the **no ip address** command. If the software detects another host using one of its IP addresses, it will print an error message on the console.

The optional **secondary** keyword allows you to specify an unlimited number of secondary addresses. Secondary addresses are treated like primary addresses, except the system never generates datagrams other than routing updates with secondary source addresses. IP broadcasts and Address Resolution Protocol (ARP) requests are handled properly, as are interface routes in the IP routing table.

Secondary IP addresses can be used in a variety of situations. The following are the most common applications:

- There may not be enough host addresses for a particular network segment. For example, your subnetting allows up to 254 hosts per logical subnet, but on one physical subnet you need 300 host addresses. Using secondary IP addresses on the devices or access servers allows you to have two logical subnets using one physical subnet.

- Many older networks were built using Level 2 bridges. The judicious use of secondary addresses can aid in the transition to a subnetted, device-based network. Devices on an older, bridged segment can be easily made aware that many subnets are on that segment.
- Two subnets of a single network might otherwise be separated by another network. This situation is not permitted when subnets are in use. In these instances, the first network is *extended*, or layered on top of the second network using secondary addresses.

**Note**

- If any device on a network segment uses a secondary address, all other devices on that same segment must also use a secondary address from the same network or subnet. Inconsistent use of secondary addresses on a network segment can very quickly cause routing loops.
- When you are routing using the Open Shortest Path First (OSPF) algorithm, ensure that all secondary addresses of an interface fall into the same OSPF area as the primary addresses.
- If you configure a secondary IP address, you must disable sending ICMP redirect messages by entering the **no ip redirects** command, to avoid high CPU utilization.

## Examples

In the following example, 192.108.1.27 is the primary address and 192.31.7.17 is the secondary address for GigabitEthernet interface 1/0/1:

```
Device# enable
Device# configure terminal
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# ip address 192.108.1.27 255.255.255.0
Device(config-if)# ip address 192.31.7.17 255.255.255.0 secondary
```

## Related Commands

| Command | Description |
|---|---|
| **match ip route-source** | Specifies a source IP address to match to required route maps that have been set up based on VRF connected routes. |
| **route-map** | Defines the conditions for redistributing routes from one routing protocol into another, or to enable policy routing. |
| **set vrf** | Enables VPN VRF selection within a route map for policy-based routing VRF selection. |
| **show ip arp** | Displays the ARP cache, in which SLIP addresses appear as permanent ARP table entries. |
| **show ip interface** | Displays the usability status of interfaces configured for IP. |
| **show route-map** | Displays static and dynamic route maps. |

# ip 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

| | |
|---|---|
| *rule* | IP admission rule name. |

## Command Default

Web authentication is disabled.

## Command Modes

Interface configuration

Fallback-profile configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## 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
```

# ip dhcp pool

To configure a Dynamic Host Configuration Protocol (DHCP) address pool on a DHCP server and enter DHCP pool configuration mode, use the **ip dhcp pool** command in global configuration mode. To remove the address pool, use the no form of this command.

**ip dhcp pool** *name*
**no ip dhcp pool** *name*

**Note** When configuring the **ip dhcp pool** command, note that it can be affected by the **ip dhcp database** command if an incorrect URL is provided. The console may hang due to multiple attempts by the DHCP service to reach the URL before it returns a failure. This is expected behavior. To prevent this issue, ensure that the correct URL, including the file name, is provided when using the **ip dhcp database** command, especially when it includes ftp/tftp.

## Syntax Description

| | |
|---|---|
| *name* | Name of the pool. Can either be a symbolic string (such as engineering) or an integer (such as 0). |

## Command Default

DHCP address pools are not configured.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(1)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

During execution of this command, the configuration mode changes to DHCP pool configuration mode, which is identified by the (config-dhcp)# prompt. In this mode, the administrator can configure pool parameters, like the IP subnet number and default router list.

## Examples

The following example configures pool1 as the DHCP address pool:

```
ip dhcp pool pool1
```

## Related Commands

| Command | Description |
|---|---|
| **host** | Specifies the IP address and network mask for a manual binding to a DHCP client. |
| **ip dhcp excluded-address** | Specifies IP addresses that a Cisco IOS DHCP server should not assign to DHCP clients. |

| Command | Description |
|---|---|
| **network (DHCP)** | Configures the subnet number and mask for a DHCP address pool on a Cisco IOS DHCP server. |

# ip dhcp-relay information option server-override

To enable the system to globally insert the server ID override and link selection suboptions into the DHCP relay agent information option in forwarded BOOTREQUEST messages to a Dynamic Host Configuration Protocol (DHCP) server, use the **ip dhcp-relay information option server-override** command in global configuration mode. To disable inserting the server ID override and link selection suboptions into the DHCP relay agent information option, use the **no** form of this command.

**ip dhcp-relay information option server-override**
**no ip dhcp-relay information option server-override**

## Syntax Description

This command has no arguments or keywords.

## Command Default

The server ID override and link selection suboptions are not inserted into the DHCP relay agent information option.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 2.1 | This command was introduced on Cisco ASR 1000 Series Aggregation Services Routers. |
| 12.2(33)SRE | This command was integrated into Cisco IOS Release 12.2(33)SRE. |
| 15.1(1)SY | This command was integrated into Cisco IOS Release 15.1(1)SY. |

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

## Usage Guidelines

The **ip dhcp-relay information option server-override** command adds the following suboptions into the relay agent information option when DHCP broadcasts are forwarded by the relay agent from clients to a DHCP server:

- Server ID override suboption
- Link selection suboption

When this command is configured, the gateway address (giaddr) will be set to the IP address of the outgoing interface, which is the interface that is reachable by the DHCP server.

If the **ip dhcp relay information option server-id-override** command is configured on an interface, it overrides the global configuration on that interface only.

## Examples

In the following example, the DHCP relay will insert the server ID override and link selection suboptions into the relay information option of the DHCP packet. The loopback interface IP address is configured to be the source IP address for the relayed messages.

```
Device(config)# ip dhcp-relay information option server-override
Device(config)# ip dhcp-relay source-interface loopback 0
Device(config)# interface Loopback 0
Device(config-if)# ip address 10.2.2.1 255.255.255.0
```

## Related Commands

| Command | Description |
|---|---|
| **ip dhcp relay information option server-id-override** | Enables the system to insert the server ID override and link selection suboptions on a specific interface into the DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server. |

# ip dhcp-relay source-interface

To globally configure the source interface for the relay agent to use as the source IP address for relayed messages, use the **ip dhcp-relay source-interface** command in global configuration mode. To remove the source interface configuration, use the **no** form of this command.

**ip dhcp-relay source-interface** *type number*
**no ip dhcp-relay source-interface** *type number*

## Syntax Description

| | |
|---|---|
| *type* | Interface type. For more information, use the question mark (?) online help function. |
| *number* | Interface or subinterface number. For more information about the numbering system for your networking device, use the question mark (?) online help function. |

## Command Default

The source interface is not configured.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 2.1 | This command was introduced on Cisco ASR 1000 Series Aggregation Services Routers. |
| 12.2(33)SRE | This command was integrated into Cisco IOS Release 12.2(33)SRE. |
| 15.1(1)SY | This command was integrated into Cisco IOS Release 15.1(1)SY. |

## Usage Guidelines

The **ip dhcp-relay source-interface** command allows the network administrator to specify a stable, hardware-independent IP address (such as a loopback interface) for the relay agent to use as a source IP address for relayed messages.

If the **ip dhcp-relay source-interface** global configuration command is configured and the **ip dhcp relay source-interface** command is also configured, the **ip dhcp relay source-interface** command takes precedence over the global configuration command. However, the global configuration is applied to interfaces without the interface configuration.

## Examples

In the following example, the loopback interface IP address is configured to be the source IP address for the relayed messages:

```
Device(config)# ip dhcp-relay source-interface loopback 0
Device(config)# interface loopback 0
Device(config-if)# ip address 10.2.2.1 255.255.255.0
```

## Related Commands

| Command | Description |
|---|---|
| **ip dhcp relay source-interface** | Configures the source interface for the relay agent to use as the source IP address for relayed messages. |

# ip domain lookup

To enable IP Domain Name System (DNS)-based hostname-to-address translation, use the **ip domain lookup** command in global configuration mode. To disable DNS-based hostname-to-address translation, use the **no** form of this command.

**ip domain lookup** [ **nsap** | **recursive** | **source-interface** *interface-type-number* | **vrf** *vrf-name* { **source-interface** *interface-type-number* } ]

## Syntax Description

| | |
|---|---|
| **nsap** | (Optional) Enables IP DNS queries for Connectionless Network Service (CLNS) and Network Service Access Point (NSAP) addresses. |
| **recursive** | (Optional) Enables IP DNS recursive lookup. |
| **source-interface** *interface-type-number* | (Optional) Specifies the source interface for the DNS resolver. Enter an interface type and number. |
| **vrf** *vrf-name* | (Optional) Defines a Virtual Routing and Forwarding (VRF) table. For vrf-name, enter a name for the VRF table. |

## Command Default

IP DNS-based hostname-to-address translation is enabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Fuji 16.9.2 | This command was introduced. |
| Cisco IOS XE Dublin 17.12.1 | An issue relating to the configuration of the **ip domain lookup source-interface** *interface-type-number* command on Layer 3 physical interfaces was resolved.<br>Starting from this release, even if configured on a Layer 3 physical interface, the command is retained across reloads and in case the port mode is changed. |

## Usage Guidelines

If this command is enabled on a device and you execute the **show tcp brief** command, the output may be displayed very slowly.

When both IP and ISO CLNS are enabled on a device, the **ip domain lookup nsap** command allows you to discover a CLNS address without having to specify a full CLNS address, given a hostname.

This command is useful for the **ping** (ISO CLNS) command, and for CLNS Telnet connections.

If you configure the **ip domain lookup source-interface** *interface-type-number* command on a Layer 3 physical interface, note the following: If the port mode is changed or in case of a device reload, the command is automatically removed from running configuration (Refer to the output of the **show running-configuration** privileged EXEC command when this happens). Removal of the command causes DNS queries that use the specified source interface, to be dropped. The only available workaround is to reconfigure the command. Starting with Cisco IOS XE Dublin 17.12.1, this issue is resolved.

## Examples

The following example shows how to configure IP DNS-based hostname-to-address translation:

```
Device# configure terminal
Device(config)# ip domain lookup
Device(config)# end
```

The following example shows how to configure a source interface for the DNS domain lookup:

```
Device# configure terminal
Device(config)# ip domain lookup source-interface gigabitethernet1/0/2
Device(config)# end
```

# ip domain-name

To configure the host domain on the device, use the **ip domain-name** command.

**ip domain-name** *domain-name* [**vrf** *vrf-name*]

## Syntax Description

| | |
|---|---|
| *domain-name* | Default domain name. |
| *vrf-name* | Specifies the virtual routing and forwarding (VRF) to use to resolve the domain name. |

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to configure a host domain in a device:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ip domain-name domain-name
```

# ip flow-export destination

To configure ETA flow export destination, use the **ip flow-export destination** command.

**ip flow-export destination** *ip_address port_number*

## Syntax Description

| | |
|---|---|
| *port_number* | Port number. The range is from 1 to 65535. |

## Command Default

None

## Command Modes

ET-Analytics configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to configure ETA flow export destination in the ET-Analytics configuration mode:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# et-analytics
Device(config-et-analytics)# ip flow-export
destination 120.0.0.1 2055
Device(config-et-analytics)# end
```

# ip helper-address

To enable forwarding of User Datagram Protocol (UDP) broadcasts, including Bootstrap Protocol (BOOTP), received on an interface, use the **ip helper-address** command in interface configuration mode. To disable forwarding of broadcast packets to specific addresses, use the**no** form of this command.

**ip helper-address**[**vrf** *name* | **global**] *address* {[**redundancy** *vrg-name*]}
**no ip helper-address** [**vrf** *name* | **global**] *address* {[**redundancy** *vrg-name*]}

## Syntax Description

| | |
|---|---|
| **vrf** *name* | (Optional) Enables the VPN routing and forwarding (VRF) instance and the VRF name. |
| **global** | (Optional) Configures a global routing table. |
| *address* | Destination broadcast or host address to be used when forwarding UDP broadcasts. There can be more than one helper address per interface. |
| **redundancy** *vrg-name* | (Optional) Defines the Virtual Router Group (VRG) name. |

## Command Default

UDP broadcasts are not forwarded.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 10.0 | This command was introduced. |
| 12.2(4)B | This command was modified. The **vrf** *name* keyword and argument pair and the **global** keyword were added. |
| 12.2(15)T | This command was modified. The **redundancy** *vrg-name* keyword and argument pair was added. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

The **ip forward-protocol** command along with the **ip helper-address** command allows you to control broadcast packets and protocols that are forwarded.

One common application that requires helper addresses is DHCP, which is defined in RFC 1531. To enable BOOTP or DHCP broadcast forwarding for a set of clients, configure a helper address on the router interface connected to the client. The helper address must specify the address of the BOOTP or DHCP server. If you have multiple servers, configure one helper address for each server.

The following conditions must be met for a UDP or IP packet to be able to use the **ip helper-address** command:

- The MAC address of the received frame must be all-ones broadcast address (ffff.ffff.ffff).

- The IP destination address must be one of the following: all-ones broadcast (255.255.255.255), subnet broadcast for the receiving interface, or major-net broadcast for the receiving interface if the **no ip classless** command is also configured.
- The IP time-to-live (TTL) value must be at least 2.
- The IP protocol must be UDP (17).
- The UDP destination port must be for TFTP, Domain Name System (DNS), Time, NetBIOS, ND, BOOTP or DHCP packet, or a UDP port specified by the **ip forward-protocol udp** command in global configuration mode.

If the DHCP server resides in a VPN or global space that is different from the interface VPN, then the **vrf** *name* or the **global** option allows you to specify the name of the VRF or global space in which the DHCP server resides.

The **ip helper-addressvrf***name address* option uses the address associated with the VRF name regardless of the VRF of the incoming interface. If the **ip helper-addressvrf***name address* command is configured and later the VRF is deleted from the configuration, then all IP helper addresses associated with that VRF name will be removed from the interface configuration.

If the **ip helper-address** *address* command is already configured on an interface with no VRF name configured, and later the interface is configured with the **ip helper-address vrf** *name address* command, then the previously configured **ip helper-address** *address* command is considered to be global.

**Note** The **ip helper-address**command does not work on an X.25 interface on a destination router because the router cannot determine if the packet was intended as a physical broadcast.

The **service dhcp** command must be configured on the router to enable IP helper statements to work with DHCP. If the command is not configured, the DHCP packets will not be relayed through the IP helper statements. The **service dhcp** command is configured by default.

## Examples

The following example shows how to define an address that acts as a helper address:

```
Router(config)# interface ethernet 1
Router(config-if)# ip helper-address 10.24.43.2
```

The following example shows how to define an address that acts as a helper address and is associated with a VRF named host1:

```
Router(config)# interface ethernet 1/0
Router(config-if)# ip helper-address vrf host1 10.25.44.2
```

The following example shows how to define an address that acts as a helper address and is associated with a VRG named group1:

```
Router(config)# interface ethernet 1/0
Router(config-if)# ip helper-address 10.25.45.2 redundancy group1
```

## Related Commands

| Command | Description |
|---|---|
| **ip forward-protocol** | Specifies which protocols and ports the router forwards when forwarding broadcast packets. |
| **service dhcp** | Enables the DHCP server and relay agent features on the router. |

# ip http authentication

To specify a particular authentication method for HTTP server users, use the **ip http authentication** command in global configuration mode. To disable a configured authentication method, use the **no** form of this command

**ip http authentication** { **aaa** { **command-authorization** *level list-name* | **exec-authorization** *list-name* | **login-authentication** *list-name* } | **enable** | **local** }

**no ip http authentication** { **aaa** { **command-authorization** *level list-name* | **exec-authorization** *list-name* | **login-authentication** *list-name* } | **enable** | **local** }

## Syntax Description

| | |
|---|---|
| **aaa** | Indicates that the authentication method used for the authentication, authorization, and accounting (AAA) login service should be used for authentication. The AAA login authentication method is specified by the **aaa authentication login default** command, unless otherwise specified by the **login-authentication** *listname* keyword and argument. |
| **command-authorization** | Sets the authorization method list for commands at the specified privilege level. |
| *level* | Indicates a privilege value from 0 through 15. By default, there are the following three command privilege levels on the router:<br>**1.** 0--Includes the **disable** , **enable** , **exit** , **help** , and **logout** commands.<br>**2.** 1--Includes all user-level commands at the device prompt (>).<br>**3.** 15--Includes all enable-level commands at the device prompt (>). |
| *list-name* | Sets the name of the method list. |
| **exec-authorization** | Sets the method list for EXEC authorization, which applies authorization for starting an EXEC session. |
| **login-authentication** | Sets the method list for login authentication, which enables AAA authentication for logins. |
| **enable** | Indicates that the "enable" password should be used for authentication. (This is the default method.) |
| **local** | ndicates that the login user name, password and privilege level access combination specified in the local system configuration (by the **username** global configuration command) should be used for authentication and authorization. |

## Command Default

None

## Command Modes

Global Configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

## Usage Guidelines

The **ip http authentication** command specifies the authentication method to be used for login when a client connects to the HTTP server. Use of the **aaa** option is recommended. The **enable**, **local**, and **tacacs** methods should be specified using the **aaa authentication login** command.

The “enable” password method is the default HTTP server authentication method. If the enable password is used as the HTTP server login authentication method, the client connects to the HTTP server with a default privilege level of 15.

## Examples

The following example shows how to specify that AAA should be used for authentication for HTTP server users. The AAA login method is configured as the “local” username/password authentication method. This example also shows how to specify using the local username database for login authentication and EXEC authorization of HTTP sessions:

```
Device(config)# ip http authentication aaa authentication login LOCALDB local
Device(config)# aaa authorization exec LOCALDB local
Device(config)# ip http authentication aaa login-authentication LOCALDB
Device(config)# ip http authentication aaa exec-authorization LOCALDB
```

# ip http auth-retry

To configure the maximum number of authentication retry attempts within a specific time-window, use the **ip http auth-retry** command.

**ip http auth-retry** *retry_number* **time-window** *time-in-minutes*

## Syntax Description

| | |
|---|---|
| *retry_number* | Specifies the maximum number of authentication retry attempts. |
| **time-window** | Retry time window in minutes. |
| *time-in-minutes* | The time window period in minutes during which the maximum number of authentication retries specified can be attempted. |

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

## Examples

The following example shows how to configure the maximum number of authentication retry attempts as 5 in a time-window of 2 minutes:

```
Device# ip http auth-retry 5 time-window 2
```

# ip http active-session-modules

To selectively enable HTTP applications that will service incoming HTTP requests from remote clients, use the **ip http active-session-modules** command. Use the **no** form of this command to return to the default, for which all HTTP services will be enabled.

**ip http active-session-modules** { *list-name* | **all** | **none** }

**no ip http active-session-modules** { *list-name* | **all** | **none** }

## Syntax Description

| | |
|---|---|
| *list-name* | Enables only those HTTP services configured in the list identified by the **ip http session-module-list** command to serve HTTP requests. All other HTTP or HTTPS applications on the controller will be disabled. |
| **all** | Enables all HTTP applications to service incoming HTTP requests from remote clients. |
| **none** | Disables all HTTP services. |

## Command Default

If no arguments or keywords are specified, all HTTP services are enabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

## Usage Guidelines

Use the **ip http active-session-modules** command to selectively enable HTTP applications, for servicing incoming HTTP requests from remote clients. With this command, a selected list of applications can be enabled. All the applications can be enabled or none of the applications can be enabled, in other words, all disabled. Use the **ip http session-module-list** command to define a list of HTTP or secure HTTP (HTTPS) application names to be enabled. If an HTTP request is made for a service that is disabled, a 404 error message is displayed in the remote client browser.

## Examples

The following example shows how to configure a different set of services to be available for HTTP and HTTPS requests. In this example, all HTTP applications are enabled for providing services to remote clients, but for HTTPS services, only the HTTPS applications defined in list1 (Simple Certificate Enrollment Protocol [SCEP] and HOME_PAGE) are enabled:

```
Device# ip http session-module-list list1 SCEP,HOME_PAGE
ip http active-session-modules all
ip http server
ip http secure-server
ip http secure-active-session-modules list1
```

# ip http client secure-ciphersuite

To specify the CipherSuite that should be used for encryption over the secure HTTP connection from the client to a remote server, use the **ip http client secure-ciphersuite** command in global configuration mode. To remove a previously configured CipherSuite specification for the client, use the **no** form of this command.

**ip http client secure-ciphersuite** [**3des-ede-cbc-sha**] [**rc4-128-sha**] [**rc4-128-md5**] [**des-cbc-sha**]
**no ip http client secure-ciphersuite**

## Syntax Description

| | |
|---|---|
| **3des-ede-cbc-sha** | SSL_RSA_WITH_3DES_EDE_CBC_SHA--Rivest, Shamir, and Adleman (RSA) key exchange with 3DES and DES-EDE3-CBC for message encryption and Secure Hash Algorithm (SHA) for message digest. |
| **rc4-128-sha** | SSL_RSA_WITH_RC4_128_SHA--RSA key exchange (RSA Public Key Cryptography) with RC4 128-bit encryption for message encryption and SHA for message digest. |
| **rc4-128-md5** | SSL_RSA_WITH_RC4_128_MD5--RSA key exchange (RSA Public Key Cryptography) with RC4 128-bit encryption for message encryption and Message Digest 5 (MD5) for message digest. |
| **des-cbc-sha** | SSL_RSA_WITH_DES_CBC_SHA--RSA key exchange with DES-CBC for message encryption and SHA for message digest. |

## Command Default

The client and server negotiate the best CipherSuite that they both support from the list of available CipherSuites.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE |

## Usage Guidelines

This command allows you to restrict the list of CipherSuites (encryption algorithms) that the client offers when connecting to a secure HTTP server. For example, you may want to allow only the most secure CipherSuites to be used.

Unless you have a reason to specify the CipherSuites that should be used, or you are unfamiliar with the details of these CipherSuites, you should leave this command unconfigured and let the server and client negotiate the CipherSuite that they both support (this is the default). The **no** form of this command returns the list of available CipherSuites to the default (that is, all CipherSuites supported on your device are available for negotiation).

## Examples

The following example shows how to configure the HTTPS client to use only the SSL_RSA_WITH_3DES_EDE_CBC_SHA CipherSuite:

```
Router(config)# ip http client secure-ciphersuite 3des-ede-cbc-sha
```

# ip http secure-ciphersuite

To specify the CipherSuites that should be used by the secure HTTP server when negotiating a connection with a remote client, use the **ip http secure-ciphersuite** command in global configuration mode. To return the configuration to the default set of CipherSuites, use the **no** form of this command.

**ip http secure-ciphersuite** [**3des-ede-cbc-sha**] [**rc4-128-sha**] [**rc4-128-md5**] [**des-cbc-sha**]
**no ip http secure-ciphersuite**

## Syntax Description

| | |
|---|---|
| **3des-ede-cbc-sha** | SSL_RSA_WITH_3DES_EDE_CBC_SHA--Rivest, Shamir, and Adleman (RSA) key exchange with 3DES and DES-EDE3-CBC for message encryption and Secure Hash Algorithm (SHA) for message digest. |
| **rc4-128-sha** | SSL_RSA_WITH_RC4_128_SHA --RSA key exchange (RSA Public Key Cryptography) with RC4 128-bit encryption for message encryption and SHA for message digest. |
| **rc4-128-md5** | SSL_RSA_WITH_RC4_128_MD5 --RSA key exchange (RSA Public Key Cryptography) with RC4 128-bit encryption for message encryption and Message Digest 5 (MD5) for message digest. |
| **des-cbc-sha** | SSL_RSA_WITH_DES_CBC_SHA--RSA key exchange with DES-CBC for message encryption and SHA for message digest. |

## Command Default

The HTTPS server negotiates the best CipherSuite using the list received from the connecting client.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE |

## Usage Guidelines

This command is used to restrict the list of CipherSuites (encryption algorithms) that should be used for encryption over the HTTPS connection. For example, you may want to allow only the most secure CipherSuites to be used.

Unless you have a reason to specify the CipherSuites that should be used, or you are unfamiliar with the details of these CipherSuites, you should leave this command unconfigured and let the server and client negotiate the CipherSuite that they both support (this is the default).

The supported CipherSuites vary by Cisco IOS software image. For example, “IP Sec56” (“k8”) images support only the SSL_RSA_WITH_DES_CBC_SHA CipherSuite in Cisco IOS Release 12.2(15)T.

In terms of router processing load (speed), the following list ranks the CipherSuites from fastest to slowest (slightly more processing time is required for the more secure and more complex CipherSuites):

1. SSL_RSA_WITH_DES_CBC_SHA
2. SSL_RSA_WITH_RC4_128_MD5
3. SSL_RSA_WITH_RC4_128_SHA

4. SSL_RSA_WITH_3DES_EDE_CBC_SHA

Additional information about these CipherSuites can be found online from sources that document the Secure Sockets Layer (SSL) 3.0 protocol.

## Examples

The following exampleshows how to restrictsthe CipherSuites offered to a connecting secure web client:

```
Router(config)# ip http secure-ciphersuite rc4-128-sha rc4-128-md5
```

# ip http secure-server

To enable a secure HTTP (HTTPS) server, enter the **ip http secure-server** command in global configuration mode. To disable the HTTPS server, use the **no** form of this command..

**ip http secure-server**
**no ip http secure-server**

## Syntax Description

This command has no arguments or keywords.

## Command Default

The HTTPS server is disabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

The HTTPS server uses the Secure Sockets Layer (SSL) version 3.0 protocol.

**Caution** When enabling an HTTPS server, you should always disable the standard HTTP server to prevent unsecured connections to the same services. Disable the standard HTTP server using the **no ip http server** command in global configuration mode (this step is precautionary; typically, the HTTP server is disabled by default).

If a certificate authority (CA) is used for certification, you should declare the CA trustpoint on the routing device before enabling the HTTPS server.

To close HTTP/TCP port 8090, you must disable both the HTTP and HTTPS servers. Enter the **no http server** and the **no http secure-server** commands, respectively.

## Examples

In the following example the HTTPS server is enabled, and the (previously configured) CA trustpoint CA-trust-local is specified:

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#ip http secure-server
Device(config)#ip http secure-trustpoint CA-trust-local
Device(config)#end

Device#show ip http server secure status
HTTP secure server status: Enabled
HTTP secure server port: 443
HTTP secure server ciphersuite: 3des-ede-cbc-sha des-cbc-sha rc4-128-md5 rc4-12a
HTTP secure server client authentication: Disabled
HTTP secure server trustpoint: CA-trust-local
```

## Related Commands

| Command | Description |
|---|---|
| **ip http secure-trustpoint** | Specifies the CA trustpoint that should be used for obtaining signed certificates for the HTTPS server. |
| **ip http server** | Enables the HTTP server on an IP or IPv6 system, including the Cisco web browser user interface. |
| **show ip http server secure status** | Displays the configuration status of the HTTPS server. |

# ip http server

To enable the HTTP server on your IP or IPv6 system, including the Cisco web browser user interface, enter the **ip http server** command in global configuration mode. To disable the HTTP server, use the **no** form of this command..

**ip http server**
**no ip http server**

## Syntax Description

This command has no arguments or keywords.

## Command Default

The HTTP server uses the standard port 80 by default.

HTTP/TCP port 8090 is open by default.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

The command enables both IPv4 and IPv6 access to the HTTP server. However, an access list configured with the **ip http access-class** command is applied only to IPv4 traffic. IPv6 traffic filtering is not supported.

**Caution** The standard HTTP server and the secure HTTP (HTTPS) server can run on a system at the same time. If you enable the HTTPS server using the **ip http secure-server** command, disable the standard HTTP server using the **no ip http server** command to ensure that secure data cannot be accessed through the standard HTTP connection.

To close HTTP/TCP port 8090, you must disable both the HTTP and HTTPS servers. Enter the **no http server** and the **no http secure-server** commands, respectively.

## Examples

The following example shows how to enable the HTTP server on both IPv4 and IPv6 systems.

After enabling the HTTP server, you can set the base path by specifying the location of the HTML files to be served. HTML files used by the HTTP web server typically reside in system flash memory. Remote URLs can be specified using this command, but use of remote path names (for example, where HTML files are located on a remote TFTP server) is not recommended.

```
Device(config)#ip http server
Device(config)#ip http path flash:
```

## Related Commands

| Command | Description |
|---|---|
| **ip http access-class** | Specifies the access list that should be used to restrict access to the HTTP server. |
| **ip http path** | Specifies the base path used to locate files for use by the HTTP server. |

| Command | Description |
|---|---|
| **ip http secure-server** | Enables the HTTPS server. |

# ip http session-module-list

To define a list of HTTP or secure HTTP application names, use the **ip http session-module-list** command in global configuration mode. To remove the defined list, use the **no** form of this command.

**ip http session-module-list** *listname prefix1* [ *prefix2,...prefixn* ]

**no ip http session-module-list** *listname prefix1* [ *prefix2,...prefixn* ]

## Syntax Description

| | |
|---|---|
| *listname* | Name of the list. |
| *prefix 1* | Associated HTTP or HTTPS application names. Prefix strings represent the names of applications, for example, SCEP, WEB_EXEC or HOME_PAGE. |
| *prefix2,...prefixn* | (Optional) Additional associated HTTP or HTTPS application names. Each application is separated by a comma. |

## Command Default

No list of HTTP or HTTPS application names is defined.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

## Usage Guidelines

Use this command to define a list of HTTP or HTTPS application names. The defined list can then be used by the **ip http active-session-modules** or **ip http secure-active-session-modules** commands to selectively enable HTTP or HTTPS applications, respectively, for servicing incoming HTTP and HTTPS requests from remote clients.

When defining a list of HTTP or HTTPS application names, use the following guidelines:

- A maximum of four lists can be defined on a controller. Attempts to define more than four lists will fail and an error message will be displayed stating the limit restrictions.
- An existing list can be removed using the **no ip http session-module-list** command.
- You cannot reconfigure an existing list. Instead of reconfiguring an existing list, remove the existing list and create a new list with the same name.
- There is no limit to how many application names can be in the list. However, the maximum number of sessions that can be registered with the Cisco IOS HTTP or HTTPS server is 32.

## Examples

The following example shows how to configure a different set of services to be available for HTTP and HTTPS requests. In this example, all HTTP applications are enabled for providing services to remote clients, but for HTTPS services, only the HTTPS applications defined in list1 (Simple Certificate Enrollment Protocol [SCEP] and HOME_PAGE) are enabled:

```
Device# ip http session-module-list list1 SCEP,HOME_PAGE
Device# ip http active-session-modules all
```

```
Device# ip http server
Device# ip http secure-server
Device# ip http secure-active-session-modules list1
```

# ip 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 | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | 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.

# ip multicast vlan

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

| | |
|---|---|
| *vlan-name* | Specifies the VLAN name. |
| *vlan-id* | Specifies the VLAN ID. |

## Command Default

Disabled.

## Command Modes

WLAN configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## 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**

## Command Default

None

## Command Modes

config-wireless-policy

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to configure 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

| | |
|---|---|
| **bootflash:** | Load the protocol pack from bootflash: |
| **force** | Force load the Load protocol pack from the selected source. |

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to 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:
```

# ip ssh

To configure Secure Shell (SSH) control parameters on your router, use the **ip ssh** command in global configuration mode. To restore the default value, use the **no** form of this command.

**ip ssh** [**timeout** *seconds* | **authentication-retries** *integer*]
**no ip ssh** [**timeout** *seconds* | **authentication-retries** *integer*]

## Syntax Description

| | |
|---|---|
| **timeout** | (Optional) The time interval that the router waits for the SSH client to respond.<br>This setting applies to the SSH negotiation phase. Once the EXEC session starts, the standard timeouts configured for the vty apply. By default, there are 5 vtys defined (0-4), therefore 5 terminal sessions are possible. After the SSH executes a shell, the vty timeout starts. The vty timeout defaults to 10 minutes. |
| *seconds* | (Optional) The number of seconds until timeout disconnects, with a maximum of 120 seconds. The default is 120 seconds. |
| **authentication- retries** | (Optional) The number of attempts after which the interface is reset. |
| *integer* | (Optional) The number of retries, with a maximum of 5 authentication retries. The default is 3. |

## Command Default

SSH control parameters are set to default router values.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.0(5)S | This command was introduced. |
| 12.1(1)T | This command was integrated into Cisco IOS Release 12.1(1) T. |
| 12.2(17a)SX | This command was integrated into Cisco IOS Release 12.2(17a)SX. |
| 12.2(33)SRA | This command was integrated into Cisco IOS release 12.(33)SRA. |
| Cisco IOS XE Release 2.4 | This command was implemented on the Cisco ASR 1000 series routers. |

## Usage Guidelines

Before you configure SSH on your router, you must enable the SSH server using the **crypto key generate rsa**command.

## Examples

The following examples configure SSH control parameters on your router:

```
ip ssh timeout 120
ip ssh authentication-retries 3
```

# ip ssh version

To specify the version of Secure Shell (SSH) to be run on a router, use the **ip ssh version**command in global configuration mode. To disable the version of SSH that was configured and to return to compatibility mode, use the **no** form of this command.

**ip ssh version** [**1** | **2**]
**no ip ssh version** [**1** | **2**]

## Syntax Description

| | |
|---|---|
| **1** | (Optional) Router runs only SSH Version 1. |
| **2** | (Optional) Router runs only SSH Version 2. |

## Command Default

If this command is not configured, SSH operates in compatibility mode, that is, Version 1 and Version 2 are both supported.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(4)T | This command was introduced. |
| 12.3(2)XE | This command was integrated into Cisco IOS Release 12.3(2)XE. |
| 12.2(25)S | This command was integrated into Cisco IOS Release 12.2(25)S. |
| 12.3(7)JA | This command was integrated into Cisco IOS Release 12.3(7)JA. |
| 12.0(32)SY | This command was integrated into Cisco IOS Release 12.0(32)SY. |
| 12.4(20)T | This command was integrated into Cisco IOS Release 12.4(20)T. |
| 15.2(2)SA2 | This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches. |

## Usage Guidelines

You can use this command with the **2** keyword to ensure that your router will not inadvertently establish a weaker SSH Version 1 connection.

## Examples

The following example shows that only SSH Version 1 support is configured:

```
Router (config)# ip ssh version 1
```

The following example shows that only SSH Version 2 is configured:

```
Router (config)# ip ssh version 2
```

The following example shows that SSH Versions 1 and 2 are configured:

```
Router (config)# no ip ssh version
```

## Related Commands

| Command | Description |
|---|---|
| debug ip ssh | Displays debug messages for SSH. |
| disconnect ssh | Terminates a SSH connection on your router. |
| **ip ssh** | Configures SSH control parameters on your router. |
| ip ssh rsa keypair-name | Specifies which RSA key pair to use for a SSH connection. |
| show ip ssh | Displays the SSH connections of your router. |

# ip tftp blocksize

To specify TFTP client blocksize, use the **ip tftp blocksize** command.

**ip tftp blocksize** *blocksize-value*

## Syntax Description

| | |
|---|---|
| *blocksize-value* | Blocksize value. Valid range is from 512-8192 Kbps. |

## Command Default

TFTP client blocksize is not configured.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

## Usage Guidelines

Use this command to change the default blocksize to decrease the image download time.

### Example

The following example shows how to specify TFTP client blocksize:

```
Device(config)# ip tftp blocksize 512
```

# ip verify source

To enable IP source guard on an interface, use the **ip verify source** command in interface configuration mode. To disable IP source guard, use the **no** form of this command.

**ip verify source**
**no ip verify source**

## Command Default

IP source guard is disabled.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

To enable IP source guard with source IP address filtering, use the **ip verify source** interface configuration command.

## Examples

This example shows how to enable IP source guard with source IP address filtering on an interface:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip verify source
```

You can verify your settings by entering the **show ip verify source** privileged EXEC command.

# ipv4 dhcp

To configure the DHCP parameters for a WLAN, use the **ipv4 dhcp** command.

**ipv4 dhcp** {**opt82** | {**ascii** | **rid** | **format** | {**ap_ethmac** | **ap_location** | **apmac** | **apname** | **policy_tag** | **ssid** | **vlan_id** }} | **required** | **server** *dhcp-ip-addr*}

## Syntax Description

| | |
|---|---|
| **opt82** | Sets DHCP option 82 for wireless clients on this WLAN |
| **required** | Specifies whether DHCP address assignment is required |
| **server** | Configures the WLAN's IPv4 DHCP Server |
| **ascii** | Supports ASCII for DHCP option 82 |
| **rid** | Supports adding Cisco 2 byte RID for DHCP option 82 |
| **format** | Sets RemoteID format |
| **ap_ethmac** | Enables DHCP AP Ethernet MAC address |
| **ap_location** | Enables AP location |
| **apmac** | Enables AP MAC address |
| **apname** | Enables AP name |
| **site_tag (Policy tag)** | Enables Site tag |
| **ssid** | Enables SSID |
| **vlan_id** | Enables VLAN ID |
| *dhcp-ip-addr* | Enter the override DHCP server's IP Address. |

## Command Default

None

## Command Modes

config-wireless-policy

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to configure DHCP address assignment as a requirement:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy demo-profile-name
Device(config-wireless-policy)# ipv4 dhcp required
```

# ipv4 flow monitor

To configure the IPv4 traffic ingress flow monitor for a WLAN profile policy, use the **ipv4 flow monitor input** command.

**ipv4 flow monitor** *monitor-name* **input**

## Syntax Description

| | |
|---|---|
| *monitor-name* | Flow monitor name. |
| **input** | Enables flow monitor on ingress traffic. |

## Command Default

None

## Command Modes

config-wireless-policy

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to configure the IPv4 traffic ingress flow monitor for a WLAN profile policy:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy policy-profile-name
Device(config-wireless-policy)# ipv4 flow monitor flow-monitor-name input
```

# ipv6 access-list

To define an IPv6 access list and to place the device in IPv6 access list configuration mode, use the **ipv6 access-list** command in global configuration mode. To remove the access list, use the **no** form of this command.

**ipv6 access-list** *access-list-name* | **match-local-traffic** | **log-update threshold** *threshold-in-msgs* | **role-based** *list-name*
**noipv6 access-list** *access-list-name* | **client** *permit-control-packets* | **log-update** *threshold* | **role-based** *list-name*

## Syntax Description

| | |
|---|---|
| **ipv6** *access-list-name* | Creates a named IPv6 ACL (up to 64 characters in length) and enters IPv6 ACL configuration mode.<br>*access-list-name* - Name of the IPv6 access list. Names cannot contain a space or quotation mark, or begin with a numeric. |
| **match-local-traffic** | Enables matching for locally-generated traffic. |
| **log-update threshold** *threshold-in-msgs* | Determines how syslog messages are generated after the initial packet match.<br>*threshold-in-msgs*- Number of packets generated. |
| **role-based** *list-name* | Creates a role-based IPv6 ACL. |

## Command Default

No IPv6 access list is defined.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

IPv6 ACLs are defined by using the **ipv6 access-list**command in global configuration mode and their permit and deny conditions are set by using the **deny** and **permit**commands in IPv6 access list configuration mode. Configuring the **ipv6 access-list**command places the device in IPv6 access list configuration mode--the device prompt changes to Device(config-ipv6-acl)#. From IPv6 access list configuration mode, permit and deny conditions can be set for the defined IPv6 ACL.

**Note** IPv6 ACLs are defined by a unique name (IPv6 does not support numbered ACLs). An IPv4 ACL and an IPv6 ACL cannot share the same name.

IPv6 is automatically configured as the protocol type in **permit any any** and **deny any any** statements that are translated from global configuration mode to IPv6 access list configuration mode.

Every IPv6 ACL has implicit **permit icmp any any nd-na**, **permit icmp any any nd-ns**, and **deny ipv6 any any** statements as its last match conditions. (The former two match conditions allow for ICMPv6 neighbor discovery.) An IPv6 ACL must contain at least one entry for the implicit **deny ipv6 any any** statement to take effect. The IPv6 neighbor discovery process makes use of the IPv6 network layer service; therefore, by default, IPv6 ACLs implicitly allow IPv6 neighbor discovery packets to be sent and received on an interface. In IPv4, the Address Resolution Protocol (ARP), which is equivalent to the IPv6 neighbor discovery process, makes use of a separate data link layer protocol; therefore, by default, IPv4 ACLs implicitly allow ARP packets to be sent and received on an interface.

Use the **ipv6 traffic-filter** interface configuration command with the *access-list-name* argument to apply an IPv6 ACL to an IPv6 interface. Use the **ipv6 access-class** line configuration command with the *access-list-name* argument to apply an IPv6 ACL to incoming and outgoing IPv6 virtual terminal connections to and from the device.

An IPv6 ACL applied to an interface with the **ipv6 traffic-filter** command filters traffic that is forwarded, not originated, by the device.

## Examples

The example configures the IPv6 ACL list named list1 and places the device in IPv6 access list configuration mode.

```
Device(config)# ipv6 access-list list1
Device(config-ipv6-acl)#
```

The following example configures the IPv6 ACL named list2 and applies the ACL to outbound traffic on Ethernet interface 0. Specifically, the first ACL entry keeps all packets from the network FEC0:0:0:2::/64 (packets that have the site-local prefix FEC0:0:0:2 as the first 64 bits of their source IPv6 address) from exiting out of Ethernet interface 0. The second entry in the ACL permits all other traffic to exit out of Ethernet interface 0. The second entry is necessary because an implicit deny all condition is at the end of each IPv6 ACL.

```
Device(config)# ipv6 access-list list2 deny FEC0:0:0:2::/64 any
Device(config)# ipv6 access-list list2 permit any any
Device(config)# interface ethernet 0
Device(config-if)# ipv6 traffic-filter list2 out
```

# ipv6 address

To configure an IPv6 address based on an IPv6 general prefix and enable IPv6 processing on an interface, use the **ipv6 address**command in interface configuration mode. To remove the address from the interface, use the **no** form of this command.

**ipv6 address** {*ipv6-prefix/prefix-length* | *prefix-name sub-bits/prefix-length*}
**no ipv6 address** {*ipv6-address/prefix-length* | *prefix-name sub-bits/prefix-length*}

## Syntax Description

| | |
|---|---|
| *ipv6-address* | The IPv6 address to be used. |
| / *prefix-length* | The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value. |
| *prefix-name* | A general prefix, which specifies the leading bits of the network to be configured on the interface. |
| *sub-bits* | The subprefix bits and host bits of the address to be concatenated with the prefixes provided by the general prefix specified with the *prefix-name* argument.<br>The *sub-bits*argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. |

## Command Default

No IPv6 addresses are defined for any interface.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(2)T | This command was introduced. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(25)SG | This command was integrated into Cisco IOS Release 12.2(25)SG. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| Cisco IOS XE Release 2.1 | This command was integrated into Cisco ASR 1000 Series devices. |
| 15.2(4)S | This command was integrated into Cisco IOS Release 15.2(4)S. |
| 15.2(2)SNG | This command was implemented on the Cisco ASR 901 Series Aggregation Services devices. |
| Cisco IOS XE Release 3.2SE | This command was integrated into Cisco IOS XE Release 3.2SE. |

## Usage Guidelines

The **ipv6 address** command allows multiple IPv6 addresses to be configured on an interface in various different ways, with varying options. The most common way is to specify the IPv6 address with the prefix length.

Addresses may also be defined using the general prefix mechanism, which separates the aggregated IPv6 prefix bits from the subprefix and host bits. In this case, the leading bits of the address are defined in a general prefix, which is globally configured or learned (for example, through use of Dynamic Host Configuration Protocol-Prefix Delegation (DHCP-PD)), and then applied using the *prefix-name* argument. The subprefix bits and host bits are defined using the *sub-bits* argument.

Using the **no ipv6 address autoconfig** command without arguments removes all IPv6 addresses from an interface.

IPv6 link-local addresses must be configured and IPv6 processing must be enabled on an interface by using the **ipv6 address link-local** command.

## Examples

The following example shows how to enable IPv6 processing on the interface and configure an address based on the general prefix called my-prefix and the directly specified bits:

```
Device(config-if) ipv6 address my-prefix 0:0:0:7272::72/64
```

Assuming the general prefix named my-prefix has the value of 2001:DB8:2222::/48, then the interface would be configured with the global address 2001:DB8:2222:7272::72/64.

## Related Commands

| Command | Description |
|---|---|
| **ipv6 address anycast** | Configures an IPv6 anycast address and enables IPv6 processing on an interface. |
| **ipv6 address eui-64** | Configures an IPv6 address and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address. |
| **ipv6 address link-local** | Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface. |
| **ipv6 unnumbered** | Enables IPv6 processing on an interface without assigning an explicit IPv6 address to the interface. |
| **no ipv6 address autoconfig** | Removes all IPv6 addresses from an interface. |
| **show ipv6 interface** | Displays the usability status of interfaces configured for IPv6. |

# ipv6 dhcp pool

To configure a Dynamic Host Configuration Protocol (DHCP) for IPv6 server configuration information pool and enter DHCP for IPv6 pool configuration mode, use the **ipv6 dhcp pool** command in global configuration mode. To delete a DHCP for IPv6 pool, use the **no** form of this command.

**ipv6 dhcp pool** *poolname*
**no ipv6 dhcp pool** *poolname*

## Syntax Description

| | |
|---|---|
| *poolname* | User-defined name for the local prefix pool. The pool name can be a symbolic string (such as "Engineering") or an integer (such as 0). |

## Command Default

DHCP for IPv6 pools are not configured.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(4)T | This command was introduced. |
| 12.2(18)SXE | This command was integrated into Cisco IOS Release 12.2(18)SXE. |
| 12.4(24)T | This command was integrated into Cisco IOS Release 12.4(24)T. |
| Cisco IOS XE Release 2.1 | This command was integrated into Cisco IOS XE Release 2.1. |
| 12.2(33)SRE | This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE. |
| 12.2(33)XNE | This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE. |

## Usage Guidelines

Use the **ipv6 dhcp pool**command to create a DHCP for IPv6 server configuration information pool. When the **ipv6 dhcp pool** command is enabled, the configuration mode changes to DHCP for IPv6 pool configuration mode. In this mode, the administrator can configure pool parameters, such as prefixes to be delegated and Domain Name System (DNS) servers, using the following commands:

- **address prefix** *IPv6-prefix* [**lifetime** {*valid-lifetime preferred-lifetime* | **infinite**}]sets an address prefix for address assignment. This address must be in hexadecimal, using 16-bit values between colons.
- **link-address** *IPv6-prefix* sets a link-address IPv6 prefix. When an address on the incoming interface or a link-address in the packet matches the specified IPv6-prefix, the server uses the configuration information pool. This address must be in hexadecimal, using 16-bit values between colons.
- **vendor-specific** *vendor-id* enables DHCPv6 vendor-specific configuration mode. Specify a vendor identification number. This number is the vendor IANA Private Enterprise Number. The range is 1 to 4294967295. The following configuration command is available:
    - **suboption** *number* sets vendor-specific suboption number. The range is 1 to 65535. You can enter an IPv6 address, ASCII text, or a hex string as defined by the suboption parameters.

**Note** The **hex** value used under the **suboption** keyword allows users to enter only hex digits (0-f). Entering an invalid **hex** value does not delete the previous configuration.

Once the DHCP for IPv6 configuration information pool has been created, use the **ipv6 dhcp server** command to associate the pool with a server on an interface. If you do not configure an information pool, you need to use the **ipv6 dhcp server interface** configuration command to enable the DHCPv6 server function on an interface.

When you associate a DHCPv6 pool with an interface, only that pool services requests on the associated interface. The pool also services other interfaces. If you do not associate a DHCPv6 pool with an interface, it can service requests on any interface.

Not using any IPv6 address prefix means that the pool returns only configured options.

The **link-address** command allows matching a link-address without necessarily allocating an address. You can match the pool from multiple relays by using multiple link-address configuration commands inside a pool.

Since a longest match is performed on either the address pool information or the link information, you can configure one pool to allocate addresses and another pool on a subprefix that returns only configured options.

## Examples

The following example specifies a DHCP for IPv6 configuration information pool named cisco1 and places the router in DHCP for IPv6 pool configuration mode:

```
Router(config)# ipv6 dhcp pool cisco1
Router(config-dhcpv6)#
```

The following example shows how to configure an IPv6 address prefix for the IPv6 configuration pool cisco1:

```
Router(config-dhcpv6)# address prefix 2001:1000::0/64
Router(config-dhcpv6)# end
```

The following example shows how to configure a pool named engineering with three link-address prefixes and an IPv6 address prefix:

```
Router# configure terminal
Router(config)# ipv6 dhcp pool engineering
Router(config-dhcpv6)# link-address 2001:1001::0/64
Router(config-dhcpv6)# link-address 2001:1002::0/64
Router(config-dhcpv6)# link-address 2001:2000::0/48
Router(config-dhcpv6)# address prefix 2001:1003::0/64
Router(config-dhcpv6)# end
```

The following example shows how to configure a pool named 350 with vendor-specific options:

```
Router# configure terminal
Router(config)# ipv6 dhcp pool 350
Router(config-dhcpv6)# vendor-specific 9
Router(config-dhcpv6-vs)# suboption 1 address 1000:235D::1
Router(config-dhcpv6-vs)# suboption 2 ascii "IP-Phone"
Router(config-dhcpv6-vs)# end
```

## Related Commands

| Command | Description |
|---|---|
| **ipv6 dhcp server** | Enables DHCP for IPv6 service on an interface. |
| **show ipv6 dhcp pool** | Displays DHCP for IPv6 configuration pool information. |

# ipv6 enable

To enable IPv6 processing on an interface that has not been configured with an explicit IPv6 address, use the **ipv6 enable**command in interface configuration mode. To disable IPv6 processing on an interface that has not been configured with an explicit IPv6 address, use the **no** form of this command.

**ipv6 enable**
**no ipv6 enable**

## Syntax Description

This command has no arguments or keywords.

## Command Default

IPv6 is disabled.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.2(2)T | This command was introduced. |
| 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(25)SG | This command was integrated into Cisco IOS Release 12.2(25)SG. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| Cisco IOS XE Release 2.1 | This command was integrated into Cisco IOS XE Release 2.1. |
| 15.2(2)SNG | This command was implemented on the Cisco ASR 901 Series Aggregation Services devices. |
| Cisco IOS XE Release 3.2SE | This command was integrated into Cisco IOS XE Release 3.2SE. |
| 15.2(2)SA2 | This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches. |

## Usage Guidelines

The **ipv6 enable**command automatically configures an IPv6 link-local unicast address on the interface while also enabling the interface for IPv6 processing. The no **ipv6 enable**command does not disable IPv6 processing on an interface that is configured with an explicit IPv6 address.

## Examples

The following example enables IPv6 processing on Ethernet interface 0/0:

```
Device(config)# interface ethernet 0/0
Device(config-if)# ipv6 enable
```

## Related Commands

| Command | Description |
|---|---|
| **ipv6 address link-local** | Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface. |
| **ipv6 address eui-64** | Configures an IPv6 address and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address. |
| **ipv6 unnumbered** | Enables IPv6 processing on an interface without assigning an explicit IPv6 address to the interface. |
| **show ipv6 interface** | Displays the usability status of interfaces configured for IPv6. |

# ipv6 mld snooping

To enable Multicast Listener Discovery version 2 (MLDv2) protocol snooping globally, use the **ipv6 mld snooping** command in global configuration mode. To disable the MLDv2 snooping globally, use the **no** form of this command.

**ipv6 mld snooping**
**no ipv6 mld snooping**

## Syntax Description

This command has no arguments or keywords.

## Command Default

This command is enabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(18)SXE | This command was introduced on the Supervisor Engine 720. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 15.4(2)S | This command was implemented on the Cisco ASR 901 Series Aggregation Services Router. |

## Usage Guidelines

MLDv2 snooping is supported on the Supervisor Engine 720 with all versions of the Policy Feature Card 3 (PFC3).

To use MLDv2 snooping, configure a Layer 3 interface in the subnet for IPv6 multicast routing or enable the MLDv2 snooping querier in the subnet.

## Examples

This example shows how to enable MLDv2 snooping globally:

```
Router(config)# ipv6 mld snooping
```

## Related Commands

| Command | Description |
|---|---|
| **show ipv6 mld snooping** | Displays MLDv2 snooping information. |

# ipv6 nd managed-config-flag

To set the managed address configuration flag in IPv6 router advertisements, use the **ipv6 nd managed-config-flag** command in an appropriate configuration mode. To clear the flag from IPv6 router advertisements, use the **no** form of this command.

**ipv6 nd managed-config-flag**
**no ipv6 nd managed-config-flag**

## Syntax Description

This command has no keywords or arguments.

## Command Default

The managed address configuration flag is not set in IPv6 router advertisements.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

## Usage Guidelines

Setting the managed address configuration flag in IPv6 router advertisements indicates to attached hosts whether they should use stateful autoconfiguration to obtain addresses. If the flag is set, the attached hosts should use stateful autoconfiguration to obtain addresses. If the flag is not set, the attached hosts should not use stateful autoconfiguration to obtain addresses.

Hosts may use stateful and stateless address autoconfiguration simultaneously.

## Examples

This example shows how to configure the managed address configuration flag in IPv6 router advertisements:

```
Device(config)# interface
Device(config-if)# ipv6 nd managed-config-flag
```

# ipv6 nd other-config-flag

To set the other stateful configuration flag in IPv6 router advertisements, use the **ipv6 nd other-config-flag** command in an appropriate configuration mode. To clear the flag from IPv6 router advertisements, use the **no** form of this command.

**ipv6 nd other-config-flag**

## Syntax Description

This command has no keywords or arguments.

## Command Default

The other stateful configuration flag is not set in IPv6 router advertisements.

## Command Modes

Interface configuration

Dynamic template configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

## Usage Guidelines

The setting of the other stateful configuration flag in IPv6 router advertisements indicates to attached hosts how they can obtain autoconfiguration information other than addresses. If the flag is set, the attached hosts should use stateful autoconfiguration to obtain the other (nonaddress) information.

**Note** If the managed address configuration flag is set using the **ipv6 nd managed-config-flag** command, then an attached host can use stateful autoconfiguration to obtain the other (nonaddress) information regardless of the setting of the other stateful configuration flag.

## Examples

This example (not applicable for BNG) configures the “other stateful configuration” flag in IPv6 router advertisements:

```
Device(config)# interface
Device(config-if)# ipv6 nd other-config-flag
```

# ipv6 nd ra throttler attach-policy

To configure a IPv6 policy for feature RA throttler, use the **ipv6 nd ra-throttler attach-policy** command.

**ipv6 nd ra-throttler attach-policy** *policy-name*

## Syntax Description

| | |
|---|---|
| **ipv6** | IPv6 root chain. |
| **ra-throttler** | Configure RA throttler on the VLAN. |
| **attach-policy** | Apply a policy for feature RA throttler. |
| *policy-name* | Policy name for feature RA throttler |

## Command Default

None

## Command Modes

config-vlan

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to configure configure a IPv6 policy for feature RA throttler:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# vlan configuration vlan-id
Device(config-vlan-config)# ipv6 nd ra-throttler attach-policy
```

# ipv6 nd raguard policy

To define the router advertisement (RA) guard policy name and enter RA guard policy configuration mode, use the **ipv6 nd raguard policy** command in global configuration mode.

**ipv6 nd raguardpolicy** *policy-name*

## Syntax Description

| | |
|---|---|
| *policy-name* | IPv6 RA guard policy name. |

## Command Default

An RA guard policy is not configured.

## Command Modes

Global configuration (config)#

## Command History

| Release | Modification |
|---|---|
| 12.2(50)SY | This command was introduced. |
| 15.2(4)S | This command was integrated into Cisco IOS Release 15.2(4)S. |
| 15.0(2)SE | This command was integrated into Cisco IOS Release 15.0(2)SE. |
| Cisco IOS XE Release 3.2SE | This command was integrated into Cisco IOS XE Release 3.2SE. |

## Usage Guidelines

Use the **ipv6 nd raguard policy** command to configure RA guard globally on a router. Once the device is in ND inspection policy configuration mode, you can use any of the following commands:

- **device-role**
- **drop-unsecure**
- **limit address-count**
- **sec-level minimum**
- **trusted-port**
- **validate source-mac**

After IPv6 RA guard is configured globally, you can use the **ipv6 nd raguard attach-policy** command to enable IPv6 RA guard on a specific interface.

## Examples

The following example shows how to define the RA guard policy name as policy1 and place the device in policy configuration mode:

```
Device(config)# ipv6 nd raguard policy policy1
Device(config-ra-guard)#
```

## Related Commands

*Table 8:*

| Command | Description |
|---|---|
| **device-role** | Specifies the role of the device attached to the port. |
| **drop-unsecure** | Drops messages with no or invalid options or an invalid signature. |
| **ipv6 nd raguard attach-policy** | Applies the IPv6 RA guard feature on a specified interface. |
| **limit address-count** | Limits the number of IPv6 addresses allowed to be used on the port. |
| **sec-level minimum** | Specifies the minimum security level parameter value when CGA options are used. |
| **trusted-port** | Configures a port to become a trusted port. |
| **validate source-mac** | Checks the source MAC address against the link layer address. |

# ipv6 traffic-filter

This command enables IPv6 traffic filter.

To enable the filtering of IPv6 traffic on an interface, use the **ipv6 traffic-filter** command. To disable the filtering of IPv6 traffic on an interface, use the **no** form of the command.

Use the **ipv6 traffic-filter** interface configuration command on the switch stack or on a standalone switch to filter IPv6 traffic on an interface. The type and direction of traffic that you can filter depends on the feature set running on the switch stack. Use the **no** form of this command to disable the filtering of IPv6 traffic on an interface.

**ipv6 traffic-filter** [**web**] *acl-name*
**no ipv6 traffic-filter** [**web**]

## Syntax Description

| | |
|---|---|
| **web** | (Optional) Specifies an IPv6 access name for the WLAN Web ACL. |
| *acl-name* | Specifies an IPv6 access name. |

## Command Default

Filtering of IPv6 traffic on an interface is not configured.

## Command Modes

wlan

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

To configure the dual IPv4 and IPv6 template, enter the **sdm prefer dual-ipv4-and-ipv6 {default | vlan}** global configuration command and reload the switch.

You can use the **ipv6 traffic-filter** command on physical interfaces (Layer 2 or Layer 3 ports), Layer 3 port channels, or switch virtual interfaces (SVIs).

You can apply an ACL to outbound or inbound traffic on Layer 3 interfaces (port ACLs), or to inbound traffic on Layer 2 interfaces (router ACLs).

If **any** port ACL (IPv4, IPv6, or MAC) is applied to an interface, that port ACL is used to filter packets, and any router ACLs attached to the SVI of the port VLAN are ignored.

This example shows how to filter IPv6 traffic on an interface:

```
Device(config-wlan)# ipv6 traffic-filter TestDocTrafficFilter
```

# key

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

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

| Command | Description |
|---|---|
| **accept-lifetime** | Sets the time period during which the authentication key on a key chain is received as valid. |
| **key chain** | Defines an authentication key chain needed to enable authentication for routing protocols. |
| **key-string (authentication)** | Specifies the authentication string for a key. |
| **show key chain** | Displays authentication key information. |

# key config-key password-encrypt

To set a private configuration key for password encryption, use the **key config-key password-encrypt** command. To disable this feature, use the **no** form of this command.

**key config-key password-encrypt** *<config-key>*

## Syntax Description

| | |
|---|---|
| *config-key* | Enter a value with minimum 8 characters.<br>**Note** The value must not begin with the following special characters:<br>!, #, and ; |

## Command Default

None

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 17.6.1 | This command was introduced. |

### Examples

The following example shows how to set a username and password for AP management:

```
Device# enable
Device# configure terminal
Device(config)# key config-key password-encryption 12345678
Device(config-ap-profile)# password encryption aes
Device(config-ap-profile)# end
```

# ldap attribute-map

To configure a dynamic attribute map on an SLDAP server, use the **ldap attribute-map** command.

**ldap** **attribute-map** *map-name*

### Command Default

None

### Command Modes

Global configuration (config)

### Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to configure 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
```

# ldap server

To configure secure LDAP, use the **ldap server** command.

**ldap server** *name*

## Syntax Description

| | |
|---|---|
| *name* | Server name. |

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

### Example

This example shows how to configure 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
```

# license air level

To configure AIR licenses on a wireless controller, enter the **license air level** command in global configuration mode. To revert to the default setting, use the **no** form of this command.

**license air level** { **air-network-advantage** [ **addon air-dna-advantage** ] | **air-network-essentials** [ **addon air-dna-essentials** ] }

**no license air level**

## Syntax Description

| | |
|---|---|
| **air-network-advantage** | Configures the AIR Network Advantage license level. |
| **addon air-dna-advantage** | (Optional) Configures the add-on AIR DNA Advantage license level.<br>This add-on option is available with the AIR Network Advantage license. |
| **air-network-essentials** | Configures the AIR Network Essentials license level. |
| **addon air-dna-essentials** | (Optional) Configures the add-on AIR DNA Essentials license level.<br>This add-on option is available with the AIR Network Essential license. |

## Command Default

For all Cisco Catalyst 9800 Wireless controllers the default license is AIR DNA Advantage.

For EWC-APs:

- Prior to Cisco IOS XE Bengaluru 17.4.1, the default license is AIR DNA Essentials.
- Starting with Cisco IOS XE Bengaluru 17.4.1, the default license is AIR Network Essentials

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |
| Cisco IOS XE Amsterdam 17.3.2a | This command continues to be available and applicable with the introduction of Smart Licensing Using Policy. |
| Cisco IOS XE Bengaluru 17.4.1 | Only for EWC-APs, the default license was changed from AIR DNA Essentials to AIR Network Essentials. |

## Usage Guidelines

In the Smart Licensing Using Policy environment, you can use the **license air level** command to change the license level being used on the product instance, or to additionally configure an add-on license on the product instance. The change is effective after a reload.

The licenses that can be configured are:

- AIR Network Essential
- AIR Network Advantage
- AIR DNA Essential

- AIR DNA Advantage

You can configure AIR DNA Essential or AIR DNA Advantage license level and on term expiry, you can move to the Network Advantage or Network Essentials license level, if you do not want to renew the DNA license.

Every connecting AP requires a Cisco DNA Center License to leverage the unique value properties of the controller.

### Examples

The following example show how to configure the AIR DNA Essential license level:

```
Device# configure terminal
Device(config)# license air level network-essentials addon air-dna-essentials
```

The following example shows how the AIR DNA Advantage license level is configured to begin with and then changed to AIR DNA Essentials:

Current configuration as AIR DNA Advantage:

```
Device# show version
Cisco IOS XE Software, Version 17.03.02
Cisco IOS Software [Amsterdam], C9800-CL Software (C9800-CL-K9_IOSXE), Version 17.3.2,
RELEASE SOFTWARE
<output truncated>
AIR License Level: AIR DNA Advantage
Next reload AIR license Level: AIR DNA Advantage

Smart Licensing Status: Registration Not Applicable/Not Applicable
<output truncated>
```

Configuration of AIR DNA Essentials :

```
Device# configure terminal
Device(config)# license air level air-network-essentials addon air-dna-essentials
```

```
Device# exit
Device# show version
Cisco IOS XE Software, Version 17.03.02
Cisco IOS Software [Amsterdam], C9800-CL Software (C9800-CL-K9_IOSXE), Version 17.3.2,
RELEASE SOFTWARE
<output truncated>
AIR License Level: AIR DNA Advantage
Next reload AIR license Level: AIR DNA Essentials
Smart Licensing Status: Registration Not Applicable/Not Applicable
<output truncated>

Device# write memory
Device# reload
```

After reload:

```
Device# show version
Cisco IOS XE Software, Version 17.03.02
Cisco IOS Software [Amsterdam], C9800-CL Software (C9800-CL-K9_IOSXE), Version 17.3.2,
RELEASE SOFTWARE
<output truncated>
AIR License Level: AIR DNA Essentials
Next reload AIR license Level: AIR DNA Essentials

Smart Licensing Status: Registration Not Applicable/Not Applicable
<output truncated>
```

# license smart (global config)

To configure licensing-related settings such as the mode of transport and the URL that the product instance uses to communicate with Cisco Smart Software Manager (CSSM), or Cisco Smart Licensing Utility (CSLU), or Smart Software Manager On-Prem (SSM On-Prem), to configure the usage reporting interval, to configure the information that must be exluded or included in a license usage report (RUM report), enter the **license smart** command in global configuration mode. Use the **no** form of the command to revert to default values.

**license smart** { **custom_id** *ID* | **enable** | **privacy** { **all** | **hostname** | **version** } | **proxy** { **address** *address_hostname* | **port** *port* } | **reservation** | **server-identity-check** | **transport** { **automatic** | **callhome** | **cslu** | **off** | **smart** } | **url** { *url* | **cslu** *cslu_or_on-prem_url* | **default** | **smart** *smart_url* | **utility** *secondary_url* } | **usage** { **customer-tags** { **tag1** | **tag2** | **tag3** | **tag4** } *tag_value* | **interval** *interval_in_days* } | **utility** [ **customer_info** { **city** *city* | **country** *country* | **postalcode** *postalcode* | **state** *state* | **street** *street* } ] }

**no license smart** { **custom_id** | **enable** | **privacy** { **all** | **hostname** | **version** } | **proxy** { **address** *address_hostname* | **port** *port* } | **reservation** | **server-identity-check** | **transport** | **url** { *url* | **cslu** *cslu_or_on-prem_url* | **default** | **smart** *smart_url* | **utility** *secondary_url* } | **usage** { **customer-tags** { **tag1** | **tag2** | **tag3** | **tag4** } *tag_value* | **interval** *interval_in_days* } | **utility** [ **customer_info** { **city** *city* | **country** *country* | **postalcode** *postalcode* | **state** *state* | **street** *street* } ] }

## Syntax Description

| | |
|---|---|
| **custom_id** *ID* | Although available on the CLI, this option is not supported. |
| **enable** | Although visible on the CLI, configuring this keyword has no effect. Smart licensing is always enabled. |

| | |
|---|---|
| **privacy** { **all** \| **hostname** \| **version** } | Sets a privacy flag to prevent the sending of the specified data privacy related information.<br>When the flag is disabled, the corresponding information is sent in a message or offline file created by the product instance.<br>Depending on the topology this is sent to one or more components, including CSSM, CSLU, and SSM On-Prem.<br>*All data privacy settings are disabled by default*. You must configure the option you want to exclude from all communication:<br>• **all**: All data privacy related information is excluded from any communication.<br>The **no** form of the command causes all data privacy related information to be sent in a message or offline file.<br>**Note** The Product ID (PID) and serial number are *included in the RUM report* regardless of whether data privacy is enabled or not.<br>• **hostname**: Excludes hostname information from any communication. When hostname privacy is enabled, the *UDI* of the product instance is displayed on the applicable user interfaces (CSSM, CSLU, and SSM On-Prem).<br>The **no** form of the command causes hostname information to be sent in a message or offline file. The hostname is displayed on the applicable user interfaces (CSSM, CSLU, and SSM On-Prem).<br>• **version**: Excludes the Cisco IOS-XE software version running on the product instance and the Smart Agent version from any communication.<br>The **no** form of the command causes version information to be sent in a message or offline file. |

| | |
|---|---|
| **proxy** { **address** *address_hostname* \| **port** *port* } | Configures a proxy for license usage synchronization with CSLU or CSSM. This means that you can use this option to configure a proxy only if the transport mode is **license smart transport smart** (CSSM), or **license smart transport cslu** (CSLU).<br>However, you cannot configure a proxy for license usage synchronization in an SSM On-Prem deployment, which also uses **license smart transport cslu** as the transport mode.<br>Configure the following options:<br>• **address** *address_hostname*: Configures the proxy address.<br>For *address_hostname*, enter the enter the IP address or hostname of the proxy.<br>• **port***port*: Configures the proxy port.<br>For *port*, enter the proxy port number. |
| **reservation** | Enables or disables a license reservation feature.<br>**Note** Although available on the CLI, this option is not applicable because license *reservation* is not applicable in the Smart Licensing Using Policy environment. |
| **server-identity-check** | Enables or disables the HTTP secure server identity check. |
| **transport** { **automatic** \| **callhome** \| **cslu** \| **off** \| **smart** } | Configures the mode of transport the product instance uses to communicate with CSSM. Choose from the following options:<br>• **automatic**: Sets the transport mode **cslu**.<br>**Note** The **automatic** keyword is not supported on Cisco Catalyst Wireless Controllers.<br>• **callhome**: Enables Call Home as the transport mode.<br>• **cslu**: Enables CSLU as the transport mode. This is the default transport mode.<br>The same keyword applies to both CSLU *and* SSM On-Prem, but the URLs are different. See **cslu***cslu_or_on-prem_url* in the following row.<br>• **off**: Disables all communication from the product instance.<br>• **smart**: Enables Smart transport. |

| |
|---|
| **url** { *url* \| **cslu** *cslu_url* \| **default** \| **smart** *smart_url* \| **utility** *secondary_url* } |

Sets URL that is used for the configured transport mode. Choose from the following options:

- *url*: If you have configured the transport mode as **callhome**, configure this option. Enter the CSSM URL exactly as follows:

  ```
  https://tools.cisco.com/its/service/oddce/services/DDCEService
  ```

  The **no license smart url** *url* command reverts to the default URL.

- **cslu** *cslu_or_on-prem_url*: If you have configured the transport mode as **cslu**, configure this option, with the URL for CSLU or SSM On-Prem, as applicable:

  - If you are using CSLU, enter the URL as follows:

    ```
    http://<cslu_ip_or_host>:8182/cslu/v1/pi
    ```

    For `<cslu_ip_or_host>`, enter the hostname or the IP address of the windows host where you have installed CSLU. 8182 is the port number and it is the only port number that CSLU uses.

    The **no license smart url cslu** *cslu_or_on-prem_url* command reverts to `http://cslu-local:8182/cslu/v1/pi`

  - If you are using SSM On-Prem, enter the URL as follows:

    ```
    http://<ip>/cslu/v1/pi/<tenant ID>
    ```

    For <ip>, enter the hostname or the IP address of the server where you have installed SSM On-Prem. The <tenantID> must be the default local virtual account ID.

    **Tip** You can retrieve the entire URL from SSM On-Prem. In the software configuration guide (17.3.x and later), see Smart Licensing Using Policy > Task Library for Smart Licensing Using Policy > Retrieving the Transport URL (SSM On-Prem UI).

    The **no license smart url cslu** *cslu_or_on-prem_url* command reverts to `http://cslu-local:8182/cslu/v1/pi`

- **default**: Depends on the configured transport mode. Only the **smart** and **cslu** transport modes are supported with this option.

  If the transport mode is set to **cslu**, and you configure **license smart url default**, the CSLU URL is configured automatically (`https://cslu-local:8182/cslu/v1/pi`).

If the transport mode is set to **smart**, and you configure **license smart url default**, the Smart URL is configured automatically (`https://smartreceiver.cisco.com/licservice/license`).

- **smart** *smart_url*: If you have configured the transport type as **smart**, configure this option. Enter the URL exactly as follows:

  ```
  https://smartreceiver.cisco.com/licservice/license
  ```

  When you configure this option, the system automatically creates a duplicate of the URL in **license smart url** *url*. You can ignore the duplicate entry, no further action is required.

  The **no license smart url smart***smart_url* command reverts to the default URL.

- **utility** *smart_url*: Although available on the CLI, this option is not supported.

| | |
|---|---|
| **usage** { **customer-tags** { **tag1** \| **tag2** \| **tag3** \| **tag4** } *tag_value* \| **interval** *interval_in_days* } | Configures usage reporting settings. You can set the following options:<br>• **customer-tags** { **tag1** \| **tag2** \| **tag3** \| **tag4** } *tag_value*: Defines strings for inclusion in data models, for telemetry. Up to 4 strings (or tags) may be defined.<br>For *tag_value*, enter the string value for each tag that you define.<br>• **interval** *interval_in_days*: Sets the reporting interval in days. By default the RUM report is sent every 30 days. The valid value range is 1 to 3650.<br>If you set the value to zero, RUM reports are not sent, regardless of what the applied policy specifies - this applies to topologies where CSLU or CSSM may be on the receiving end.<br>If you set a value that is greater than zero and the transport type is set to **off**, then, between the *interval_in_days* and the policy value for `Ongoing reporting frequency(days):`, the lower of the two values is applied. For example, if *interval_in_days* is set to 100, and the value in the in the policy says `Ongoing reporting frequency (days):90`, RUM reports are sent every 90 days.<br>If you do not set an interval, and the default is effective, the reporting interval is determined entirely by the policy value. For example, if the default value is effective and only unenforced licenses are in use, if the policy states that reporting is not required, then RUM reports are not sent. |
| **utility** [ **customer_info** { **city** *city* \| **country** *country* \| **postalcode** *postalcode* \| **state** *state* \| **street** *street* } ] | Although visible on the CLI, this option is not supported. |

## Command Default

Cisco IOS XE Amsterdam 17.3.1 or earlier: Smart Licensing is enabled by default.

Cisco IOS XE Amsterdam 17.3.2a and later: Smart Licensing Using Policy is enabled by default.

## Command Modes

Global config (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

| Release | Modification |
|---|---|
| Cisco IOS XE Amsterdam 17.3.2a | The following keywords and variables were introduced with Smart Licensing Using Policy:<br>• Under the **url**keyword, these options were introduced:<br>{ **cslu** *cslu_url* \| **smart** *smart_url* }<br>• Under the **transport** keyword, these options were introduced:<br>{ **cslu** \| **off** }<br>Further, the default transport type was changed from **callhome**, to **cslu**.<br>• **usage** { **customer-tags** { **tag1** \| **tag2** \| **tag3** \| **tag4** } *tag_value* \| **interval** *interval_in_days* }<br>The following keywords and variables under the **license smart** command are deprecated and no longer available on the CLI: **enable**and **conversion automatic**. |
| Cisco IOS XE Amsterdam 17.3.3 | SSM On-Prem support was introduced. For product instance-initiated communication in an SSM On-Prem deployment, the existing [**no** ]**license smart url cslu***cslu_or_on-prem_url* command supports the configuration of a URL for SSM On-Prem as well. But the required URL format for SSM On-Prem is: `http://<ip>/cslu/v1/pi/<tenant ID>`.<br>The corresponding transport mode that must be configured is also an existing command (**license smart transport cslu**). |
| Cisco IOS XE Cupertino 17.9.1 | • A new mechanism to send all data privacy related information was introduced. This information is no longer included in a RUM report.<br>If data privacy is disabled (**no license smart privacy** {**all** \| **hostname** \| **version**} global configuration command), data privacy related information is sent in a separate sync message or offline file.<br>• Support for sending hostname information was introduced.<br>If the privacy setting for the hostname is disabled (**no license smart privacy hostname** global configuration command), hostname information is sent from the product instance, in a separate sync message, or offline file. Depending on the topology you have implemented, the hostname information is received by CSSM, CSLU, or SSM On-Prem. It is also displayed on the corresponding user interface. |

## Usage Guidelines

### Data Privacy Settings

When you disable a privacy setting, the topology you have implemented determines the recipient and how the information reaches its destination:

- The recipient of the information may be one or more of the following: CSSM, CSLU, and SSM On-Prem. The privacy setting has no effect on a controller (Cisco DNA Center).

In case of the **hostname** keyword, after the hostname information is received by CSSM, CSLU, or SSM On-Prem, it is also displayed on the corresponding UIs – as applicable. If you then *enable* privacy the corresponding UIs revert to displaying the UDI of the product instance.

- How the information is sent.
  - In case of a topology where the product instance initiates communication, the product instance initiates the sending of this information in a message, to CSSM, or CSLU, or SSM On-Prem.

    The product instance sends the hostname sent every time one of the following events occur: the product instance boots up, the hostname changes, there is a switchover in a High Availability set-up.
  - In case of a topology where CSLU or SSM On-Prem initiate communication, the corresponding component initiates the retrieval of privacy information from the product instance.

    The hostname is retrieved at the frequency you configure in CSLU or SSM On-Prem, to retrieve information.
  - In case of a topology where the product instance is in an air-gapped network, privacy information is included in the offline file that is generated when you enter the **license smart save usage** privileged EXEC command.

**Note** For all topologies, data privacy related information is *not* included in the RUM report.

Data privacy related information it is not stored by the product instance *prior* to sending or saving. This ensures that if and when information is sent, it is consistent with the data privacy setting at the time of sending or saving.

### Communication failures and reporting

The reporting interval that you configure (**license smart usage interval** *interval_in_days* command), determines the date and time at which the product instance sends out the RUM report. If the scheduled interval coincides with a communication failure, the product instance attempts to send out the RUM report for up to four hours after the scheduled time has expired. If it is still unable to send out the report (because the communication failure persists), the system resets the interval to 15 minutes. Once the communication failure is resolved, the system reverts the reporting interval to the value that you last configured.

The system message you may see in case of a communicatin failure is %SMART_LIC-3-COMM_FAILED. For information about resolving this error and restoring the reporting interval value, in the software configuration guide of the required release (17.3.x onwards), see *System Configuration* > *Smart Licensing Using Policy* > *Troubleshooting Smart Licensing Using Policy*.

## Examples

- Examples for Data Privacy, on page 390
- Examples for Transport Type and URL, on page 390
- Examples for Usage Reporting Options, on page 391

### Examples for Data Privacy

The following examples show how to configure data privacy related information using **license smart privacy** command in global configuration mode. The accompanying **show license status** output displays configured information.

**Note** The output of the **show** command only tells you if a particular option is enabled or disabled.

Here, no data privacy related information information is sent:

```
Device# configure terminal
Device(config)# license smart privacy all
Device(config)# exit
Device# show license status
<output truncated>
Data Privacy:
  Sending Hostname: no
    Callhome hostname privacy: ENABLED
    Smart Licensing hostname privacy: ENABLED
  Version privacy: ENABLED

Transport:
  Type: Callhome
<output truncated>
```

### Examples for Transport Type and URL

The following examples show how to configure some of the transport types using the **license smart transport** and the **license smart url** commands in global configuration mode. The accompanying **show license all** output displays configured information.

Transport **cslu**:

```
Device# configure terminal
Device(config)# license smart transport cslu
Device(config)# license smart url default
Device(config)# exit
Device# show license all
<output truncated>
Transport:
  Type: cslu
  Cslu address: http://192.168.0.1:8182/cslu/v1/pi
  Proxy:
    Not Configured
<output truncated>
```

Transport **smart**:

```
Device# configure terminal
Device(config)# license smart transport smart
Device(config)# license smart url smart https://smartreceiver.cisco.com/licservice/license
Device(config)# exit
Device# show license all
<output truncated>
Transport:
  Type: Smart
  URL: https://smartreceiver-stage.cisco.com/licservice/license
  Proxy:
    Not Configured
<output truncated>
```

### Examples for Usage Reporting Options

The following examples show how to configure some of the usage reporting settings using the **license smart usage** command in global configuration mode. The accompanying **show running-config** output displays configured information.

Configuring the **customer-tag** option:

```
Device# configure terminal
Device(config)# license smart usage customer-tags tag1 SA/VA:01
Device(config)# exit
Device# show running-config | include tag1
license smart usage customer-tags tag1 SA/VA:01
```

Configuring a narrower reporting interval than the currently applied policy:

```
Device# show license status
<output truncated>
Usage Reporting:
Last ACK received: Sep 22 13:49:38 2020 PST
Next ACK deadline: Dec 21 12:02:21 2020 PST
Reporting push interval: 30 days
Next ACK push check: Sep 22 12:20:34 2020 PST
Next report push: Oct 22 12:05:43 2020 PST
Last report push: Sep 22 12:05:43 2020 PST
Last report file write: <none>
<output truncated>

Device# configure terminal
Device(config)# license smart usage interval 20
Device(config)# exit
Device# show license status
<output truncated>

Usage Reporting:
Last ACK received: Sep 22 13:49:38 2020 PST
Next ACK deadline: Nov 22 12:02:21 2020 PST
Reporting push interval: 20 days
Next ACK push check: Sep 22 12:20:34 2020 PST
Next report push: Oct 12 12:05:43 2020 PST
Last report push: Sep 22 12:05:43 2020 PST
Last report file write: <none>
<output truncated>
```

# license smart (privileged EXEC)

To configure licensing functions such as requesting or returning authorization codes, saving Resource Utilization Measurement reports (RUM reports), importing a file on to a product instance, establishing trust with Cisco Smart Software Manager (CSSM), synchronizing the product instance with CSSM, or Cisco Smart License Utility (CSLU), or Smart Software Manager On-Prem (SSM On-Prem), and removing licensing information from the product instance, enter the **license smart** command in privileged EXEC mode with the corresponding keyword or argument.

**license smart** { **authorization** { **request** { **add** | **replace** } *feature_name* { **all** | **local** } | **return** { **all** | **local** } { **offline** [ *filepath_filename* ] | **online** } } | **clear eventlog** | **export return** { **all** | **local** } *feature_name* | **factory reset** | **import** *filepath_filename* | **save** { **trust-request** *filepath_filename* | **usage** { **all** | **days** *days* | **rum-id** *rum-ID* | **unreported** } { **file** *filepath_filename* } } | **sync** { **all** | **local** } | **trust idtoken** *id_token_value* { **local** | **all** } [ **force** ] }

## Syntax Description

| | |
|---|---|
| **smart** | Provides options for Smart Licensing. |
| **authorization** | Provides the option to request for, or return, authorization codes.<br>Authorization codes are required *only* if you use licenses with enforcement type: export-controlled or enfored. |
| **request** | Requests an authorization code from CSSM, CSLU (CSLU in-turn fetches it from CSSM), or SSM On-Prem and installs it on the product instance. |
| **add** | Adds the requested license to the existing authorization code. The new authorization code will contain all the licenses of the existing authorization code and the requested license. |
| **replace** | Replaces the existing authorization code. The new authorization code will contain only the requested license. All licenses in the current authorization code are returned.<br>When you enter this option, the product instance verifies if licenses that correspond to the authorization codes that will be removed, are in-use. If licenses are being used, an error message tells you to first disable the corresponding features. |
| *feature_name* | Name of the license for which you are requesting an authorization code. |
| **all** | Performs the action for all product instances in a High Availability configuration. |
| **local** | Performs the action for the *active* product instance. This is the default option. |
| **return** | Returns an authorization code back to the license pool in CSSM. |
| **offline** *filepath_filename* | Means the product instance is not connected to CSSM. The authorization code is returned offline. This option requires you to print the return code to a file.<br>Optionally, you can also specify a path to save the file. The file format can be any readable format, such as `.txt`<br>If you choose the offline option, you must complete the additional step of copying the return code from the CLI or the saved file and entering it in CSSM. |

| | |
|---|---|
| **online** | Means that the product instance is in a connected mode. The authorization code is returned to CSLU or CSSM directly. |
| **clear eventlog** | Clears all event log files from the product instance. |
| **export return** | Returns the authorization key for an export-controlled license. |
| **factory reset** | Clears all saved licensing information from the product instance. |
| **import** *filepath_filename* | Imports a file on to the product instance. The file may be that of an authorization code, a trust code, or, or a policy.<br>For *filepath_filename*, specify the location, including the filename. |
| **save** | Provides options to save RUM reports or trust code requests. |
| **trust-request** *filepath_filename* | Saves the trust code request for the active product instance in the specified location.<br>For *filepath_filename*, specify the absolute path to the file, including the filename. |
| **usage** { **all** \| **days** *days* \| **rum-id** *rum-ID* \| **unreported** } { **file** *file_path* } | Saves RUM reports (license usage information) in the specified location. You must specify one of these options:<br>• **all**: Saves all RUM reports.<br>• **days** *days*: Saves RUM report for the last *n* number of days (excluding the current day). Enter a number. The valid range is 0 to 4294967295.<br>For example, if you enter 3, RUM reports of the last three days are saved.<br>• **rum-Id** *rum-ID*: Saves a specified RUM ID. The valid value range is 0 to 18446744073709551615.<br>• **unreported**: Saves all unreported RUM reports.<br>**file** *filepath_filename*: Saves the specified usage information to a file. Specify the absolute path to the file, including the filename. |
| **sync** { **all** \| **local** } | Synchronizes with CSSM or CSLU, or SSM On-Prem, to send and receive any pending data. This includes uploading pending RUM reports, downloading the ACK response, any pending authorization codes, trust codes, and policies for the product instance.<br>Specify the product instance by entering one of these options:<br>• **all**: Performs synchronization for all the product instances in a High Availability set-up. If you choose this option, the product instance also sends the list of all the UDIs in the synchronization request.<br>• **local**: Performs synchronization only for the active product instance sending the request, that is, its own UDI. This is the default option. |
| **trust idtoken** *id_token_value* | Establishes a trusted connection with CSSM.<br>To use this option, you must first generate a token in the CSSM portal. Provide the generated token value for *id_token_value*. |

| | |
|---|---|
| **force** | Submits a trust code request even if a trust code already exists on the product instance.<br>A trust code is node-locked to the UDI of a product instance. If the UDI is already registered, CSSM does not allow a new registration for the same UDI. Entering the **force** keyword overrides this behavior. |

## Command Default

Cisco IOS XE Amsterdam 17.3.1 or earlier: Smart Licensing is enabled by default.

Cisco IOS XE Amsterdam 17.3.2a and later: Smart Licensing Using Policy is enabled by default.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |
| Cisco IOS XE Amsterdam 17.3.2a | The following keywords and variables were introduced with Smart Licensing Using Policy:<br>• **authorization** { **request** { **add** \| **replace** } *feature_name* { **all** \| **local** } \| **return** { **all** \| **local** } { **offline** [ *path* ] \| **online** } }<br>• **import** *file_path*<br>• **save** { **trust-request** *filepath_filename* \| **usage** { **all** \| **days** *days* \| **rum-id** *rum-ID* \| **unreported** } { **file** *file_path* } }<br>• **sync** { **all** \| **local** }<br>• **trust idtoken** *id_token_value* { **local** \| **all** } [ **force** ]<br>The following keywords and variables under the **license smart** command are deprecated and no longer available on the CLI:<br>• **register idtoken** *token_id* [ **force** ]<br>• **renew id** { **ID** \| **auth** }<br>• **debug** { **error** \| **debug** \| **trace** \| **all** }<br>• **reservation** { **cancel** [ **all** \| **local** ] \| **install** [ **file** ] *key* \| **request** { **all** \| **local** \| **universal** } \| **return** [ **all** \| **authorization** { *auth_code* \| **file** *filename* } \| **Local** ] *key* }<br>• **mfg reservation** { **request** \| **install** \| **install file** \| **cancel** }<br>• **conversion** { **start** \| **stop** } |
| Cisco IOS XE Amsterdam 17.3.3 | Support for SSM On-Prem was introduced. You can perform licensing-related tasks such as saving Resource Utilization Measurement reports (RUM reports), importing a file on to a product instance, synchronizing the product instance, returning authorization codes, and removing licensing information from the product instance in an SSM On-Prem deployment. |

## Usage Guidelines

### Overwriting a Trust Code

Use case for the **force** option when configuring the **license smart trust idtoken** command: You use same token for all the product instances that are part of one Virtual Account. If the product instance has moved from one account to another (for instance, because it was added to a High Availability set-up, which is part of another Virtual Account), then there may be an existing trust code you have to overwrite.

### Removing Licensing Information

Entering the **licence smart factory reset** command removes all licensing information (except the licenses in-use) from the product instance, including any authorization codes, RUM reports etc. Therefore, we recommend the use of this command only if the product instance is being returned (Return Material Authrization, or RMA), or being decommissioned permanently. We also recommend that you send a RUM report to CSSM, before you remove licensing information from the product instance - this is to ensure that CSSM has up-to-date usage information.

### Authorization Codes and License Reservations:

Options relating to authorization codes and license reservations:

- Since there are no export-controlled or enforced licenses on any of the Cisco Catalyst Wireless Controllers, and the notion of reserved licenses is not applicable in the Smart Licensing Using Policy environment, the following commands are not applicable:
  - { { **license smart authorization request** { **add** | **replace** | **save** *path* } *feature_name* { **all** | **local** } *request_count* } }
  - **license smart export return**
- The following option is applicable and required for any SLR authorization codes you may want to return:

  **license smart authorization return** { **all** | **local** } { **offline** [ *path* ] | **online** }

## Examples

- Example for Saving Licensing Usage Information, on page 395
- Example for Installing a Trust Code, on page 396
- Example for Returning an SLR Authorization Code, on page 396

## Example for Saving Licensing Usage Information

The following example shows how you can save license usage information on the product instance. You can use this option to fulfil reporting requirements in an air-gapped network. In the example, the file is first save to flash memory and then copied to a TFTP location:

```
 Device> enable
Device# license smart save usage unreported file flash:RUM-unrep.txt
Device# dir
Directory of bootflash:/

33      -rw-             5994   Nov 2 2020 03:58:04 +05:00  RUM-unrep.txt

Device# copy flash:RUM-unrep.txt tftp://192.168.0.1//auto/tftp-user/user01/
Address or name of remote host [192.168.0.1]?
Destination filename [//auto/tftp-user/user01/RUM-unrep.txt]?
```

```
!!
15128 bytes copied in 0.161 secs (93963 bytes/sec)
```

After you save RUM reports to a file, you must upload it to CSSM (from a workstation that has connectivity to the internet, and Cisco).

### Example for Installing a Trust Code

The following example shows how to install a trust code even if one is already installed on the product instance. This requires connectivity to CSSM. The accompanying **show license status** output shows sample output after successful installation:

Before you can install a trust code, you must generate a token and download the corresponding file from CSSM.

Use the **show license status** command (`Trust Code Installed:`) to verify results.

```
Device> enable
Device# license smart trust idtoken
NGMwMjk5mYtNZaxMS00NzMZmtgWm local force

Device# show license status
<output truncated>
Trust Code Installed:
  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
    INSTALLED on Nov 02 05:19:05 2020 IST
  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
    INSTALLED on Nov 02 05:19:05 2020 IST
<output truncated>
```

### Example for Returning an SLR Authorization Code

The following example shows how to remove and return an SLR authorization code. Here the code is returned offline (no connectivity to CSSM). The accompanying **show license all** output shows sample output after successful return:

```
Device> enable
Device# show license all
<output truncated>
License Authorizations
======================
Overall status:
  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
      Status: SPECIFIC INSTALLED on Nov 02 03:16:01 2020 IST
      Last Confirmation code: 102fc949
  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
      Status: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
      Last Confirmation code: ad4382fe
<output truncated>

Device# license smart authorization return local offlline
Enter this return code in Cisco Smart Software Manager portal:
UDI: PID:C9800-CL-K9,SN:93BBAH93MGS
    Return code: CqaUPW-WSPYiq-ZNU2ci-SnWydS-hBCXHP-MuyPqy-PJ1GiG-tPTGQj-S2h
UDI: PID:C9800-CL-K9,SN:9XECPSUU4XN
    Return code: CNLwxR-eWiAEJ-XaTEQg-j4rrYW-dSRz9j-37VpcP-imjuLD-mNeA4k-TXA

Device# show license all
<output truncated>
```

```
License Authorizations
======================
Overall status:
  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
      Status: NOT INSTALLED
      Last return code: CqaUPW-WSPYiq-ZNU2ci-SnWydS-hBCXHP-MuyPqy-PJ1GiG-tPTGQj-S2h
  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
      Status: NOT INSTALLED
      Last return code: CNLwxR-eWiAEJ-XaTEQg-j4rrYW-dSRz9j-37VpcP-imjuLD-mNeA4k-TXA
<output truncated>
```

If you choose the **offline** option, you must complete the additional step of copying the return code from the CLI or the saved file and entering it in CSSM.

# line vty

To identify a specific line for configuration and begin the command in line configuration mode in a virtual terminal for remote console access, use the **line vty** command.

**line vty** *line_number*

## Syntax Description

| | |
|---|---|
| *line_number* | First line number. Valid values range from 0 to 530. |

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

## Examples

The following example shows how to identify a specific line for configuration in a virtual terminal:

```
Device# line vty 10
```

# local-auth ap eap-fast

To configure Flex policy local authentication using EAP Fast method, use the **local-auth ap eap-fast** command.

**local-auth ap eap-fast** *profile-name*

## Syntax Description

| | |
|---|---|
| *profile-name* | Enter eap-fast profile name. |

## Command Default

None

## Command Modes

config-wireless-flex-profile

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to configure EAP Fast method authentication on a Flex policy:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile flex profile-name
Device(config-wireless-flex-profile)# local-auth ap eap-fast eap-fast-profile-name
```

# local-site

To configure the site as local site, use the **local-site** command.

**local-site**

## Syntax Description

| | |
|---|---|
| **local-site** | Configure this site as local site. |

## Command Default

None

## Command Modes

config-site-tag

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to set the current site as local site:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless tag site tag-name
Device(config-site-tag)# local-site
```

# location expiry

To configure the location expiry duration, use the **location expiry** command in global configuration mode.

**location expiry** {**calibrating-client** | **client** | **tags** }*timeout-duration*

## Syntax Description

| | |
|---|---|
| **calibrating-client** | Timeout value for calibrating clients. |
| **client** | Timeout value for clients. |
| **tags** | Timeout value for RFID tags. |
| *timeout-duration* | Timeout duration, in seconds. |

## Command Default

Timeout value is not configured.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

### Example

This example shows how to configure the location expiry duration:

```
Device(config)# location expiry tags 50
```

# location notify-threshold

To configure the NMSP notification threshold for RSSI measurements, use the **location notify-threshold** command in global configuration mode. To remove the NMSP notification threshold for RSSI measurements, use the **no** form of this command.

**location notify-threshold** {**client** | **rogue-aps** | **tags** } *db*
**no location notify-threshold** {**client** | **rogue-aps** | **tags** }

## Syntax Description

| | |
|---|---|
| **client** | Specifies the NMSP notification threshold (in dB) for clients and rogue clients.<br>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.<br>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.<br>The valid range for the threshold parameter is 0 to 10 dB, and the default value is 0 dB. |
| *db* | The valid range for the threshold parameter is 0 to 10 dB, and the default value is 0 dB. |

## Command Default

No default behavior or values.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to configure the NMSP notification threshold to 10 dB for clients. A notification NMSP message is sent to MSE as soon as the client RSSI changes by 10 dB:

```
Device# configure terminal
Device(config)# location notify-threshold client 10
Device(config)# end
```

# login authentication

To configure login authentication parameters, use the **login authentication** command.

**login authentication** *word* **default**

## Syntax Description

| | |
|---|---|
| *word* | Authentication list with a name. |
| **default** | Uses the default authentication list. |

## Command Default

None

## Command Modes

Line configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

## Examples

The following example shows how to configure login authentication :

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# line console 0
Device(config-line)# login authentication NO_LOGIN
```

# login block-for

To configure the login security on the Cisco controller and to set the duration for which the controller has to block further login attempts after a specified number of consecutive failed login attempts within a certain time frame, use the **login block-for** command.

**login block-for** *duration* **attempts** *attempts* **within** *time-frame*

## Syntax Description

| | |
|---|---|
| *duration* | Specifies the duration in seconds for which the device will block login attempts |
| **attempts** | Number of consecutive failed login attempts |
| *attempts* | Specifies the maximum number of failed attempts |
| **within** | Time frame within which the specified number of consecutive failed login attempts must occur to trigger the blocking |
| *time-frame* | Specifies the time period in seconds |

## Command Default

None

## Command Modes

Global Configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

## Examples

The following example shows how to configure the login security on the controller to set the duration of 60 seconds for which the controller has to block further login attempts after 3 unsuccessful login attempts within a period of 10 seconds.:

```
Device# login block-for 60 attempts 3 within 10
```

# lsc-only-auth (mesh)

To configure mesh security to Locally Significant Certificate (LSC) only MAP authentication, use the **lsc-only-auth** command.

**lsc-only-auth**

## Syntax Description

This command has no keywords or arguments.

## Command Default

LSC only authentication is enabled.

## Command Modes

config-wireless-mesh-profile

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

### Example

The following example shows how to configure mesh 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* ]

### Syntax Description

| | |
|---|---|
| *mac-authorization-list* | Name of the Authorization list. |

### Command Default

None

### Command Modes

config-wlan

### Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to enable MAC filtering on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan-name wlan-index SSID-name
Device(config-wlan)# mac-filtering
```

# mab request format attribute

To configure the delimiter while configuring MAC filtering on a WLAN, use the **mab request format attribute** command in global configuration mode. To disable the delimiter while configuring MAC filtering on a WLAN, use the **no** form of this command.

**mab request format attribute** { **1 groupsize** *size* **separator** *separator* [ **lowercase** | **uppercase** ] | **2** { **0** | **7** | **LINE** } **LINE** *password* | **32 vlan access-vlan** }

**no mab request format attribute** { **1 groupsize** *size* **separator** *separator* [ **lowercase** | **uppercase** ] | **2** { **0** | **7** | **LINE** } **LINE** *password* | **32 vlan access-vlan** }

## Syntax Description

| | |
|---|---|
| **1** | Specifies the username format used for MAB requests. |
| **groupsize** *size* | Specifies the number of hex digits per group.<br>The valid values range from 1 to 12. |
| **separator** *separator* | Specifies how to separate groups.<br>The separators are hyphen (-), colon (:), and full stop (.)<br>For more information about the groupsize and separator, refer to the Overview of the Configurable MAB Username and Password. |
| **lowercase** | Specifies the username in lowercase format. |
| **uppercase** | Specifies the username in uppercase format. |
| **2** | Specifies the global password used for all the MAB requests. |
| **0** | Specifies the unencrypted password. |
| **7** | Specifies the hidden password. |
| **LINE** | Specifies the encrypted or unencrypted password. |
| *password* | LINE password. |
| **32** | Specifies the NAS-Identifier attribute. |
| **vlan** | Specifies a VLAN. |
| **access-vlan** | Specifies the configured access VLAN. |

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Example:

The following example shows how to configure the delimiter while configuring MAC filtering:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# mab request format attribute 1 groupsize 4 separator -
```

# match (access-map configuration)

To set the VLAN map to match packets against one or more access lists, use the **match** command in access-map configuration mode on the switch stack or on a standalone switch. To remove the match parameters, use the **no** form of this command.

**match** { **ip** **address** { *name number* } [ *name number* ] [ *name number* ] . . . | **ipv6** **address** { *name number* } [ *name number* ] [ *name number* ] . . . | **mac** **address** { *name* } [ *name* ] [ *name* ] . . . }
**no** **match** { **ip** **address** { *name number* } [ *name number* ] [ *name number* ] . . . | **ipv6** **address** { *name number* } [ *name number* ] [ *name number* ] . . . | **mac** **address** { *name* } [ *name* ] [ *name* ] . . . }

## Syntax Description

| | |
|---|---|
| **ip address** | Sets the access map to match packets against an IP address access list. |
| **ipv6 address** | Sets the access map to match packets against an IPv6 address access list. |
| **mac address** | Sets the access map to match packets against a MAC address access list. |
| *name* | Name of the access list to match packets against. |
| *number* | Number of the access list to match packets against. This option is not valid for MAC access lists. |

## Command Default

The default action is to have no match parameters applied to a VLAN map.

## Command Modes

Access-map configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

You enter access-map configuration mode by using the **vlan access-map** global configuration command.

You must enter one access list name or number; others are optional. You can match packets against one or more access lists. Matching any of the lists counts as a match of the entry.

In access-map configuration mode, use the **match** command to define the match conditions for a VLAN map applied to a VLAN. Use the **action** command to set the action that occurs when the packet matches the conditions.

Packets are matched only against access lists of the same protocol type; IP packets are matched against IP access lists, IPv6 packets are matched against IPv6 access lists, and all other packets are matched against MAC access lists.

IP, IPv6, and MAC addresses can be specified for the same map entry.

This example shows how to define and apply a VLAN access map vmap4 to VLANs 5 and 6 that will cause the interface to drop an IP packet if the packet matches the conditions defined in access list al2:

```
Device(config)# vlan access-map vmap4
Device(config-access-map)# match ip address al2
Device(config-access-map)# action drop
Device(config-access-map)# exit
Device(config)# vlan filter vmap4 vlan-list 5-6
```

You can verify your settings by entering the **show vlan access-map** privileged EXEC command.

# match activated-service-template

To create a condition that evaluates true based on the service template activated on a session, use the **match activated-service-template** command in control class-map filter configuration mode. To create a condition that evaluates true if the service template activated on a session does not match the specified template, use the **no-match activated-service-template** command in control class-map filter configuration mode. To remove the condition, use the **no** form of this command.

**match activated-service-template** *template-name*
**no-match activated-service-template** *template-name*
**no** {**match** | **no-match**} **activated-service-template** *template-name*

## Syntax Description

| | |
|---|---|
| *template-name* | Name of a configured service template as defined by the **service-template** command. |

## Command Default

The control class does not contain a condition based on the service template.

## Command Modes

Control class-map filter configuration (config-filter-control-classmap)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.2SE | This command was introduced. |

## Usage Guidelines

The **match activated-service-template** command configures a match condition in a control class based on the service template applied to a session. A control class can contain multiple conditions, each of which will evaluate as either true or false. The control class defines whether all, any, or none of the conditions must evaluate true for the actions of the control policy to be executed.

The **no-match** form of this command specifies a value that results in an unsuccessful match. All other values of the specified match criterion result in a successful match. For example, if you configure the **no-match activated-service-template SVC_1** command, all template values except SVC_1 are accepted as a successful match.

The **class** command associates a control class with a control policy.

## Examples

The following example shows how to configure a control class that evaluates true if the service template named VLAN_1 is activated on the session:

```
class-map type control subscriber match-all CLASS_1
 match activated-service-template VLAN_1
```

## Related Commands

| Command | Description |
|---|---|
| **activate** (policy-map action) | Activates a control policy or service template on a subscriber session. |
| **class** | Associates a control class with one or more actions in a control policy. |
| **match service-template** | Creates a condition that evaluates true based on an event’s service template. |

| Command | Description |
|---|---|
| **service-template** | Defines a template that contains a set of service policy attributes to apply to subscriber sessions. |

# match any

To perform a match on any protocol that passes through the device, use the **match any** command.

**match any**

## Command Default

None

## Command Modes

config-cmap

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to match any packet passing through the device:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# class-map cmap-name
Device(config-cmap)# match any
```

# match 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

| Release | Modification |
|---|---|
| 15.0(1)M | This command was introduced. |
| 15.2(2)T | This command was integrated into Cisco IOS Release 15.2(2)T for Cisco Performance Monitor. |
| Cisco IOS XE Release 3.5S | This command was integrated into Cisco IOS XE Release 3.5S for Cisco Performance Monitor. |

## 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
```

## Related Commands

| Command | Description |
|---|---|
| **collect application name** | Configures the use of application name as a nonkey field for a Flexible NetFlow flow record. |
| **flow record** | Creates a flow record, and enters Flexible NetFlow flow record configuration mode. |
| **flow record type performance-monitor** | Creates a flow record, and enters Performance Monitor flow record configuration mode. |

# 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## 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 419. |
| **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 421. |
| **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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## 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.

**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 419. |
| **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 421. |
| **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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## 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 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## 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.

**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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## 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 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**

## 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## 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 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**

## 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## 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.

**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 427. |
| **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 431. |

## Command Default

The IPv6 fields are not configured as a key field.

## Command Modes

Flow record configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## 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

| | |
|---|---|
| **destination address** | Configures the IPv4 destination address as a key field. For more information see match ipv6 destination address, on page 427. |
| **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 431. |

## Command Default

The IPv6 fields are not configured as a key field.

## Command Modes

Flow record configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

### Usage Guidelines

Multiple service maps of the same name with different sequence numbers can be created, and the evaluation of the filters will be ordered on the sequence number. Service lists are an ordered sequence of individual statements, with each one having a permit or deny result. The evaluation of a service list consists of a list scan in a predetermined order, and an evaluation of the criteria of each statement that matches. A list scan is stopped once the first statement match is found and a permit/deny action associated with the statement match is performed. The default action after scanning through the entire list is to deny.

**Note** It is not possible to use the **match** command if you have used the **service-list mdns-sd** *service-list-name* **query** command. The **match** command can be used only for the **permit** or **deny** option.

### Example

The following example shows how to set the announcement message type to be matched:

```
Device(config-mdns-sd-sl)# match message-type announcement
```

# match non-client-nrt

To match non-client NRT (non-real-time), use the **match non-client-nrt** command in class-map configuration mode. Use the **no** form of this command to return to the default setting.

**match non-client-nrt**
**no match non-client-nrt**

## Syntax Description

This command has no arguments or keywords.

## Command Default

None

## Command Modes

Class-map

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

None

This example show how you can configure non-client NRT:

```
Device(config)# class-map test_1000
Device(config-cmap)# match non-client-nrt
```

# match protocol

To configure the match criterion for a class map on the basis of a specified protocol, use the **match protocol** command in class-map configuration or policy inline configuration mode. To remove the protocol-based match criterion from the class map, use the **no** form of this command. For more information about the **match protocol** command, refer to the *Cisco IOS Quality of Service Solutions Command Reference*.

**match protocol** {*protocol-name* | **attribute category** *category-name* | **attribute sub-category** *sub-category-name* | **attribute application-group** *application-group-name*}

## Syntax Description

| | |
|---|---|
| *protocol-name* | Name of the protocol (for example, bgp) used as a matching criterion. |
| *category-name* | Name of the application category used as a matching criterion. |
| *sub-category-name* | Name of the application subcategory used as a matching criterion. |
| *application-group-name* | Name of the application group as a matching criterion. When the application name is specified, the application is configured as the match criterion instead of the application group. |

## Command Default

No match criterion is configured.

## Command Modes

Class-map configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to create class maps with apply match protocol filters for application name, category, and sub category:

```
Device# configure terminal
Device(config)# class-map cat-browsing
Device(config-cmap)# match protocol attribute category browsing
Device(config-cmap)#end

Device# configure terminal
Device(config)# class-map cat-fileshare
Device(config-cmap)# match protocol attribute category file-sharing
Device(config-cmap)#end

Device# configure terminal
Device(config)# class-map match-any subcat-terminal
Device(config-cmap)# match protocol attribute sub-category terminal
Device(config-cmap)#end

Device# configure terminal
Device(config)# class-map match-any webex-meeting
Device(config-cmap)# match protocol webex-meeting
Device(config-cmap)#end
```

This example shows how to create policy maps and define existing class maps for upstream QoS:

```
Device# configure terminal
Device(config)# policy-map test-avc-up
Device(config-pmap)# class cat-browsing
Device(config-pmap-c)# police 150000
Device(config-pmap-c)# set dscp 12
Device(config-pmap-c)#end


Device# configure terminal
Device(config)# policy-map test-avc-up
Device(config-pmap)# class cat-fileshare
Device(config-pmap-c)# police 1000000
Device(config-pmap-c)# set dscp 20
Device(config-pmap-c)#end


Device# configure terminal
Device(config)# policy-map test-avc-up
Device(config-pmap)# class subcat-terminal
Device(config-pmap-c)# police 120000
Device(config-pmap-c)# set dscp 15
Device(config-pmap-c)#end

Device# configure terminal
Device(config)# policy-map test-avc-up
Device(config-pmap)# class webex-meeting
Device(config-pmap-c)# police 50000000
Device(config-pmap-c)# set dscp 21
Device(config-pmap-c)#end
```

This example shows how to create policy maps and define existing class maps for downstream QoS:

```
Device# configure terminal
Device(config)# policy-map test-avc-down
Device(config-pmap)# class cat-browsing
Device(config-pmap-c)# police 200000
Device(config-pmap-c)# set dscp 10
Device(config-pmap-c)#end


Device# configure terminal
Device(config)# policy-map test-avc-up
Device(config-pmap)# class cat-fileshare
Device(config-pmap-c)# police 300000
Device(config-pmap-c)# set wlan user-priority 2
Device(config-pmap-c)# set dscp 20
Device(config-pmap-c)#end


Device# configure terminal
Device(config)# policy-map test-avc-up
Device(config-pmap)# class subcat-terminal
Device(config-pmap-c)# police 100000
Device(config-pmap-c)# set dscp 25
Device(config-pmap-c)#end

Device# configure terminal
Device(config)# policy-map test-avc-up
Device(config-pmap)# class webex-meeting
Device(config-pmap-c)# police 60000000
Device(config-pmap-c)# set dscp 41
Device(config-pmap-c)#end
```

This example shows how to apply defined QoS policy on a WLAN:

```
Device# configure terminal
Device(config)#wlan  alpha
Device(config-wlan)#shut
Device(config-wlan)#end
Device(config-wlan)#service-policy client input test-avc-up
Device(config-wlan)#service-policy client output test-avc-down
Device(config-wlan)#no shut
Device(config-wlan)#end
```

# match service-instance

To set a service instance to match a service list, use the **match service-instance** command.

**match service-instance** *line*

## Syntax Description

| | |
|---|---|
| *line* | Regular expression to match the service instance in packets. |

## Command Default

None

## Command Modes

Service list configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

It is not possible to use the **match** command if you have used the **service-list mdns-sd** *service-list-name* **query** command. The **match** command can be used only for the **permit** or **deny** option.

### Example

The following example shows how to set the service instance to match:

```
Device(config-mdns-sd-sl)# match service-instance servInst 1
```

# match service-type

To set the value of the mDNS service type string to match, use the **match service-type** command.

**match service-type** *line*

## Syntax Description

| | |
|---|---|
| *line* | Regular expression to match the service type in packets. |

## Command Default

None

## Command Modes

Service list configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

It is not possible to use the **match** command if you have used the **service-list mdns-sd** *service-list-name* **query** command. The **match** command can be used only for the **permit** or **deny** option.

### Example

The following example shows how to set the value of the mDNS service type string to match:

```
Device(config-mdns-sd-sl)# match service-type _ipp._tcp
```

# match 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

| | |
|---|---|
| **destination-port** | Configures the transport destination port as a key field. |
| **source-port** | Configures the transport source port as a key field. |

## Command Default

The transport fields are not configured as a key field.

## Command Modes

Flow record configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## 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

| | |
|---|---|
| **destination-port** | Configures the transport destination port as a key field. |
| **source-port** | Configures the transport source port as a key field. |

## Command Default

The transport fields are not configured as a key field.

## Command Modes

Flow record configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## 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

| | |
|---|---|
| **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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## 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*

### Command Default

None

### Command Modes

config-filter-control-classmap

### Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to configure a class-map attribute filter criteria:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# class-map type control subscriber match-any map-name
Device(config-filter-control-classmap)# match user-role user-role
```

# match username

To create a condition that evaluates true based on an event’s username, use the **match username** command in control class-map filter configuration mode. To create a condition that evaluates true if an event’s username does not match the specified username, use the **no-match username** command in control class-map filter configuration mode. To remove the condition, use the **no** form of this command.

**match username** *username*
**no-match username** *username*
**no** {**match** | **no-match**} **username** *username*

## Syntax Description

| | |
|---|---|
| *username* | Username. |

## Command Default

The control class does not contain a condition based on the event’s username.

## Command Modes

Control class-map filter configuration (config-filter-control-classmap)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.2SE | This command was introduced. |

## Usage Guidelines

The **match username** command configures a match condition in a control class based on the username. A control class can contain multiple conditions, each of which will evaluate as either true or false. The control class defines whether all, any, or none of the conditions must evaluate true to execute the actions of the control policy.

The **no-match** form of this command specifies a value that results in an unsuccessful match. All other values of the specified match criterion result in a successful match. For example, if you configure the **no-match username josmithe** command, the control class accepts any username value except josmithe as a successful match.

The **class** command associates a control class with a control policy.

## Examples

The following example shows how to configure a control class that evaluates true if the username is josmithe:

```
class-map type control subscriber match-all CLASS_1
 match username josmithe
```

## Related Commands

| Command | Description |
|---|---|
| **class** | Associates a control class with one or more actions in a control policy. |
| **policy-map type control subscriber** | Defines a control policy for subscriber sessions |

# match 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

You enter access-map configuration mode by using the **vlan access-map** global configuration command.

You must enter one access list name or number; others are optional. You can match packets against one or more access lists. Matching any of the lists counts as a match of the entry.

In access-map configuration mode, use the **match** command to define the match conditions for a VLAN map applied to a VLAN. Use the **action** command to set the action that occurs when the packet matches the conditions.

Packets are matched only against access lists of the same protocol type; IP packets are matched against IP access lists, and all other packets are matched against MAC access lists.

Both IP and MAC addresses can be specified for the same map entry.

## Examples

This example shows how to define and apply a VLAN access map *vmap4* to VLANs 5 and 6 that will cause the interface to drop an IP packet if the packet matches the conditions defined in access list *al2*.

```
Device(config)# vlan access-map vmap4
Device(config-access-map)# match ip address al2
Device(config-access-map)# action drop
Device(config-access-map)# exit
Device(config)# vlan filter vmap4 vlan-list 5-6
```

You can verify your settings by entering the **show vlan access-map** privileged EXEC command.

# match (class-map configuration)

To define the match criteria to classify traffic, use the **match** command in class-map configuration mode. Use the **no** form of this command to remove the match criteria.

### Cisco IOS XE Everest 16.5.x and Earlier Releases

**match** {**access-group** {**name***acl-name acl-index*} | **class-map** *class-map-name* | **cos** *cos-value* | **dscp** *dscp-value* | [ **ip** ] **dscp** *dscp-list* | [**ip**] **precedence** *ip-precedence-list* | **precedence** *precedence-value1...value4* | **qos-group** *qos-group-value* | **vlan** *vlan-id*}
**no match** {**access-group** {**name***acl-name acl-index*} | **class-map** *class-map-name* | **cos** *cos-value* | **dscp** *dscp-value* | [ **ip** ] **dscp** *dscp-list* | [**ip**] **precedence** *ip-precedence-list* | **precedence** *precedence-value1...value4* | **qos-group** *qos-group-value* | **vlan** *vlan-id*}

### Cisco IOS XE Everest 16.6.x and Later Releases

**match** {**access-group** {**name** *acl-name acl-index*} | **cos** *cos-value* | **dscp** *dscp-value* | [ **ip** ] **dscp** *dscp-list* | [ **ip** ] **precedence** *ip-precedence-list* | **mpls** *experimental-value* | **non-client-nrt** | **precedence** *precedence-value1...value4* | **protocol** *protocol-name* | **qos-group** *qos-group-value* | **vlan** *vlan-id* | **wlan** *wlan-id*}
**no match** {**access-group** {**name** *acl-name acl-index*} | **cos** *cos-value* | **dscp** *dscp-value* | [ **ip** ] **dscp** *dscp-list* | [ **ip** ] **precedence** *ip-precedence-list* | **mpls** *experimental-value* | **non-client-nrt** | **precedence** *precedence-value1...value4* | **protocol** *protocol-name* | **qos-group** *qos-group-value* | **vlan** *vlan-id* | **wlan** *wlan-id*}

## Syntax Description

| | |
|---|---|
| **access-group** | Specifies an access group. |
| **name** *acl-name* | Specifies the name of an IP standard or extended access control list (ACL) or MAC ACL. |
| *acl-index* | Specifies the number of an IP standard or extended access control list (ACL) or MAC ACL. For an IP standard ACL, the ACL index range is 1 to 99 and 1300 to 1999. For an IP extended ACL, the ACL index range is 100 to 199 and 2000 to 2699. |
| **class-map** *class-map-name* | Uses a traffic class as a classification policy and specifies a traffic class name to use as the match criterion. |
| **cos** *cos-value* | Matches a packet on the basis of a Layer 2 class of service (CoS)/Inter-Switch Link (ISL) marking. The cos-value is from 0 to 7. You can specify up to four CoS values in one **match cos** statement, separated by a space. |
| **dscp** *dscp-value* | Specifies the parameters for each DSCP value. You can specify a value in the range 0 to 63 specifying the differentiated services code point value. |

| | |
|---|---|
| **ip dscp** *dscp-list* | Specifies a list of up to eight IP Differentiated Services Code Point (DSCP) values to match against incoming packets. Separate each value with a space. The range is 0 to 63. You also can enter a mnemonic name for a commonly used value. |
| **ip precedence** *ip-precedence-list* | Specifies a list of up to eight IP-precedence values to match against incoming packets. Separate each value with a space. The range is 0 to 7. You also can enter a mnemonic name for a commonly used value. |
| **precedence** *precedence-value1...value4* | Assigns an IP precedence value to the classified traffic. The range is 0 to 7. You also can enter a mnemonic name for a commonly used value. |
| **qos-group** *qos-group-value* | Identifies a specific QoS group value as a match criterion. The range is 0 to 31. |
| **vlan** *vlan-id* | Identifies a specific VLAN as a match criterion. The range is 1 to 4094. |
| **mpls** *experimental-value* | Specifies Multi Protocol Label Switching specific values. |
| **non-client-nrt** | Matches a non-client NRT (non-real-time). |
| **protocol** *protocol-name* | Specifies the type of protocol. |
| **wlan** *wlan-id* | Identifies 802.11 specific values. |

## Command Default

No match criteria are defined.

## Command Modes

Class-map configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introc |

## Usage Guidelines

The **match** command is used to specify which fields in the incoming packets are examined to classify the packets. Only the IP access group or the MAC access group matching to the Ether Type/Len are supported.

If you enter the **class-map match-any***class-map-name* global configuration command, you can enter the following **match** commands:

- **match access-group name** *acl-name*

**Note** The ACL must be an extended named ACL.

- **match ip dscp** *dscp-list*
- **match ip precedence** *ip-precedence-list*

The **match access-group** *acl-index* command is not supported.

To define packet classification on a physical-port basis, only one **match** command per class map is supported. In this situation, the **match-any** keyword is equivalent.

For the **match ip dscp** *dscp-list* or the **match ip precedence** *ip-precedence-list* command, you can enter a mnemonic name for a commonly used value. For example, you can enter the **match ip dscp af11** command, which is the same as entering the **match ip dscp 10** command. You can enter the **match ip precedence critical** command, which is the same as entering the **match ip precedence 5** command. For a list of supported mnemonics, enter the **match ip dscp ?** or the **match ip precedence ?** command to see the command-line help strings.

Use the **input-interface** *interface-id-list* keyword when you are configuring an interface-level class map in a hierarchical policy map. For the *interface-id-list*, you can specify up to six entries.

## Examples

This example shows how to create a class map called class2, which matches all the incoming traffic with DSCP values of 10, 11, and 12:

```
Device(config)# class-map class2
Device(config-cmap)# match ip dscp 10 11 12
Device(config-cmap)# exit
```

This example shows how to create a class map called class3, which matches all the incoming traffic with IP-precedence values of 5, 6, and 7:

```
Device(config)# class-map class3
Device(config-cmap)# match ip precedence 5 6 7
Device(config-cmap)# exit
```

This example shows how to delete the IP-precedence match criteria and to classify traffic using acl1:

```
Device(config)# class-map class2
Device(config-cmap)# match ip precedence 5 6 7
Device(config-cmap)# no match ip precedence
Device(config-cmap)# match access-group acl1
Device(config-cmap)# exit
```

This example shows how to specify a list of physical ports to which an interface-level class map in a hierarchical policy map applies:

```
Device(config)# class-map match-any class4
Device(config-cmap)# match cos 4
Device(config-cmap)# exit
```

This example shows how to specify a range of physical ports to which an interface-level class map in a hierarchical policy map applies:

```
Device(config)# class-map match-any class4
Device(config-cmap)# match cos 4
Device(config-cmap)# exit
```

You can verify your settings by entering the **show class-map** privileged EXEC command.

# match wlan user-priority

To match 802.11 specific values, use the **match wlan user-priority** command in class-map configuration mode. Use the **no** form of this command to return to the default setting.

**match wlan user-priority** *wlan-value* [*wlan-value*] [*wlan-value*] [*wlan-value*]
**no match wlan user-priority** *wlan-value* [*wlan-value*] [*wlan-value*] [*wlan-value*]

## Syntax Description

| | |
|---|---|
| *wlan-value* | The 802.11-specific values. Enter the user priority 802.11 TID user priority (0-7). (Optional) Enter up to three user priority values separated by white-spaces. |

## Command Default

None

## Command Modes

Class-map configuration (config-cmap)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

None

This example show how you can configure user-priority values:

```
Device(config)# class-map test_1000
Device(config-cmap)# match wlan user-priority 7
```

# max-bandwidth

To configure the wireless media-stream's maximum expected stream bandwidth in Kbps, use the **max-bandwidth** command.

**max-bandwidth** *bandwidth*

## Syntax Description

| | |
|---|---|
| *bandwidth* | Maximum Expected Stream Bandwidth in Kbps. Valid range is 1 to 35000 Kbps. |

## Command Default

None

## Command Modes

media-stream

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to configure wireless media-stream bandwidth in Kbps:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless media-stream group doc-grp 224.0.0.0 224.0.0.223
Device(config-media-stream)# max-bandwidth 3500
```

# max-through

To limit multicast router advertisements (RAs) per VLAN per throttle period, use the **max-through** command in IPv6 RA throttle policy configuration mode. To reset the command to its defaults, use the **no** form of this command.

**max-through** {*mt-value* | **inherit** | **no-limit**}

## Syntax Description

| | |
|---|---|
| *mt-value* | Number of multicast RAs allowed on the VLAN before throttling occurs. The range is from 0 through 256. |
| **inherit** | Merges the setting between target policies. |
| **no-limit** | Multicast RAs are not limited on the VLAN. |

## Command Default

10 RAs per VLAN per 10 minutes

## Command Modes

IPv6 RA throttle policy configuration (config-nd-ra-throttle)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.2XE | This command was introduced. |

## Usage Guidelines

The **max-through** command limits the amount of multicast RAs that are passed through to the VLAN per throttle period. This command can be configured only on a VLAN.

### Example

```
Device(config)# ipv6 nd ra-throttle policy policy1
Device(config-nd-ra-throttle)# max-through 25
```

# mdns-sd

To configure the mDNS service discovery gateway, use the **mdns-sd** command. To disable the configuration, use the **no** form of this command.

**mdns-sd** { **gateway** | **service-definition** *service-definition-name* | **service-list** *service-list-name* { **IN** | **OUT** } | **service-policy** *service-policy-name* }

**no mdns-sd** { **gateway** | **service-definition** *service-definition-name* | **service-list** *service-list-name* { **IN** | **OUT** } | **service-policy** *service-policy-name* }

## Syntax Description

| | |
|---|---|
| **mdns-sd** | Configures the mDNS service discovery gateway. |
| **gateway** | Configures mDNS gateway. |
| **service-definition** | Configures mDNS service definition. |
| *service-definition-name* | Specifies the mDNS service definition name. |
| **service-list** | Configures mDNS service list. |
| *service-list-name* | Specifies the mDNS service definition name. |
| **IN** | Specifies the inbound filtering. |
| **OUT** | Specifies the outbound filtering. |
| **service-policy** | Configures mDNS service policy. |
| *service-policy-name* | Specifies the mDNS service policy name. |

## Command Default

None

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Amsterdam 17.3.1 | This command was introduced. |

## Usage Guidelines

None

### Example

The following example shows how to configure the mDNS service discovery gateway:

```
Device(config)# mdns-sd gateway
```

# mdns-sd flex-profile

To configure the mDNS service discovery flex profile, use the **mdns-sd flex-profile** command. To disable the command, use the **no** form of this command.

**mdns-sd flex-profile** *flex-profile-name*

**no mdns-sd flex-profile** *flex-profile-name*

**Syntax Description**

| | |
|---|---|
| **mdns-sd flex-profile** | Configures the mDNS service discovery flex profile. |
| *flex-profile-name* | Specifies the mDNS flex profile name. |

**Command Default**

None

**Command Modes**

Global configuration

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS XE Amsterdam 17.3.1 | This command was introduced. |

**Usage Guidelines**

None

### Example

The following example shows how to configure the mDNS service discovery flex profile:

```
Device(config)# mdns-sd flex-profile mdns-flex-profile
```

# mdns-sd profile

To apply the mDNS flex profile to the wireless flex profile, use the **mdns-sd profile** command in the wireless flex profile mode. To disable the command, use the **no** form of this command.

**mdns-sd profile** *flex-profile-name*

**no mdns-sd profile** *flex-profile-name*

## Syntax Description

| | |
|---|---|
| **mdns-sd profile** | Configures the mDNS flex profile in the wireless flex profile. |
| *flex-profile-name* | Specifies the mDNS flex profile name. |

## Command Default

None

## Command Modes

Wireless flex profile configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Amsterdam 17.3.1 | This command was introduced. |

## Usage Guidelines

None

### Example

The following example shows how to apply the mDNS flex profile to the wireless flex profile:

```
Device(config-wireless-flex-profile)# mdns-sd profile mdns-flex-profile
```

# method (mesh)

To configure authentication and authorization method for a mesh AP profile, use the **method** command.

**method** { **authentication** | **authorization** } *method*

## Syntax Description

| | |
|---|---|
| **authentication** | AAA method for mesh AP authentication. |
| **authorization** | AAA method for mesh AP authorization. |
| *method* | Named method list. |

## Command Default

Authentication and authorization method is not configured.

## Command Modes

config-wireless-mesh-profile

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

### Example

The following example shows how to configure 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to enable EAP Fast method on a EAP profile:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# eap profile profile-name
Device(config-eap-profile)# method fast
```

# mgmtuser username

To set a username and password for AP management, use the **mgmtuser username** command. To disable this feature, use the **no** form of this command.

**mgmtuser username** *username* **password {0 | 8}** *password*

## Syntax Description

| | |
|---|---|
| *username* | Enter a username for AP management. |
| *0* | Specifies an UNENCRYPTED password. |
| *8* | Specifies an AES encrypted password. |
| *password* | Configures the encryption password (key). |

## Command Default

None

## Command Modes

AP Profile Configuration (config-ap-profile)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 17.6.1 | This command was introduced. |

### Examples

The following example shows how to set a username and password for AP management:

```
Device# enable
Device# configure terminal
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# mgmtuser username myusername password 0
Device(config-ap-profile)# end
```

# mobility anchor

To configure mobility sticky anchoring, use the **mobility anchor** command. To disable the mobility 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*
**no mobility anchor** *ip-address*

## Syntax Description

|  |  |
|---|---|
| *ip-address* | Configures the IP address for the guest anchor. |

## Command Default

None

## Command Modes

Wireless policy configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to configure guest anchoring:

```
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)# mobility anchor 209.165.200.224
```

This example shows how to configure the device as an auto-anchor:

```
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)# mobility anchor
```

# monitor capture (access list/class map)

To configure a monitor capture specifying an access list or a class map as the core filter for the packet capture, use the **monitor capture** command in privileged EXEC mode. To disable the monitor capture with the specified access list or class map as the core filter, use the **no** form of this command.

**monitor capture** *capture-name* { **access-list** *access-list-name* | **class-map** *class-map-name* }

**no monitor capture** *capture-name* { **access-list** *access-list-name* | **class-map** *class-map-name* }

## Syntax Description

| | |
|---|---|
| *capture-name* | The name of the capture. |
| **access-list** *access-list-name* | Configures an access list with the specified name. |
| **class-map** *class-map-name* | Configures a class map with the specified name. |

## Command Default

A monitor capture with the specified access list or a class map as the core filter for the packet capture is not configured.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.7S | This command was introduced. |

## Usage Guidelines

Configure the access list using the **ip access-list** command or the class map using the **class-map** command before using the **monitor capture** command. You can specify a class map, or an access list, or an explicit inline filter as the core filter. If you have already specified the filter when you entered the **monitor capture match** command, the command replaces the existing filter.

## Examples

The following example shows how to define a core system filter using an existing access control list:

```
Device> enable
Device# configure terminal
Device(config)# ip access-list standard acl1
Device(config-std-nacl)# permit any
Device(config-std-nacl)# exit
Device(config)# exit
Device# monitor capture mycap access-list acl1
Device# end
```

The following example shows how to define a core system filter using an existing class map:

```
Device> enable
Device# configure terminal
Device(config)# ip access-list standard acl1
Device(config-std-nacl)# permit any
Device(config-std-nacl)# exit
Device(config)# class-map match-all cmap
Device(config-cmap)# match access-group name acl
Device(config-cmap)# exit
Device(config)# exit
Device# monitor capture mycap class-map classmap1
Device# end
```

# monitor capture export

To store captured packets in a file, use the **monitor capture export** command in privileged EXEC mode.

**monitor** **capture** *capture-name* **export** *filelocation* / *file-name*

## Syntax Description

| | |
|---|---|
| *capture-name* | Name of the capture. |
| **export** | Stores all the packets in capture buffer to a file of type .PCAP. |
| *file-location/file-name* | Destination file location and name. |

## Command Default

The captured packets are not stored.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.12.1 | This command was introduced. |

## Usage Guidelines

Use the **monitor capture export** command only when the storage destination is a capture buffer. The file may be stored either remotely or locally. Use this command either during capture or after the packet capture has stopped. The packet capture could have stopped because one or more end conditions has been met or you entered the **monitor capture stop** command.

## Examples

The following example shows how to export capture buffer contents:

```
Device> enable
Device# monitor capture mycap export tftp://10.1.88.9/mycap.pcap
Device# end
```

# monitor capture (interface/control plane)

To configure monitor capture specifying an attachment point and the packet flow direction, use the **monitor capture** command in privileged EXEC mode. To disable the monitor capture with the specified attachment point and the packet flow direction, use the **no** form of this command.

**monitor capture** *capture-name* { **interface** *type number* | **control-plane** } { **in** | **out** | **both** }
**no monitor capture** *capture-name* { **interface** *type number* | **control-plane** } { **in** | **out** | **both** }

## Syntax Description

| | |
|---|---|
| *capture-name* | Name of the capture. |
| **interface** *type number* | Configures an interface with the specified type and number as an attachment point. |
| **control-plane** | Configures a control plane as an attachment point. |
| **in** | Specifies the inbound traffic direction. |
| **out** | Specifies the outbound traffic direction. |
| **both** | Specifies both inbound and outbound traffic directions. |

## Command Default

The monitor packet capture filter specifying is not configured.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.12.1 | This command was introduced. |

## Usage Guidelines

Repeat the **monitor capture** command as many times as required to add multiple attachment points.

## Examples

The following example shows how to add an attachment point to an interface:

```
Device> enable
Device# monitor capture mycap interface GigabitEthernet 0/0/1 in
Device# end
```

The following example shows how to add an attachment point to a control plane:

```
Device> enable
Device# monitor capture mycap control-plane out
Device# end
```

# monitor capture limit

To configure capture limits, use the **monitor capture limit** command in privileged EXEC mode. To remove the capture limits, use the **no** form of this command.

**monitor capture** *capture-name* **limit** [ **duration** *seconds* ] [ **every** *number* ] [ **packet-length** *size* ] [ **packets** *number* ] [ **pps** *number* ]
**no monitor capture** *name* **limit** [ **duration** ] [ **every** ] [ **packet-length** ] [ **packets** ] [ **pps** ]

## Syntax Description

| | |
|---|---|
| *capture-name* | Name of the packet capture. |
| **duration** *seconds* | (Optional) Specifies the duration of the capture, in seconds. The range is from 1 to 1000000. |
| **every** *number* | (Optional) Specifies that, in a series of packets, the packet whose numerical order is denoted by the *number* argument should be captured. The range is from 2 to 100000. |
| **packet-length** *bytes* | (Optional) Specifies the packet length, in bytes. If the actual packet is longer than the specified length, only the first set of bytes whose number is denoted by the *bytes* argument is stored. |
| **packets** *packets-number* | (Optional) Specifies the number of packets to be processed for capture. |
| **pps** *pps-number* | (Optional) Specifies the number of packets to be captured per second. The range is from 1 to 1000000. |

## Command Default

No capture limits are configured.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.12.1 | This command was introduced. |

## Usage Guidelines

If no duration is specified, the capture does not stop until it is manually interrupted. The entire packet is processed if the **packet-length** *bytes* keyword-argument pair is not specified. All matched packets are captured, if the **every** *number* keyword-argument pair is not specified. All matched packets are captured if the **packets** *packets-number* keyword-argument pair is not specified. The incoming packets are captured at the rate of 1 million packets per second if the **pps** *number* keyword-argument pair is not specified.

## Examples

The following example shows how to specify capture limits:

```
Device> enable
Device# monitor capture mycap limit duration 10
Device# monitor capture mycap limit packet-length 128
Device# monitor capture mycap limit packets 100
Device# monitor capture mycap limit pps 1000
```

```
Device# monitor capture mycap limit duration 10 packet-length 128 packets 100
Device# end
```

# monitor capture match

To define an explicit inline core filter, use the **monitor capture match** command in privileged EXEC mode. To remove this filter, use the **no** form of this command.

**monitor capture** *capture-name* **match**
{ **any** | { **ipv4** | **ipv6** } { *source-prefix/length* | **any** | **host** } *source-ip-address* { {
*destination-prefix/length* | **any** | **host** } *destination-ip-address* } | **protocol** { **tcp** | **udp** } { {
*source-prefix/length* | **any** | **host** } { { *destination-prefix/length* | **any** | **host** } | [ [ **eq** | **gt** | **lt** |
**neg** ] *port-number* ] | **range** *start-port-number end-port-number* | [ **eq** | **gt** | **lt** | **neg** ]
*port-number* | **range** *start-port-number end-port-number* } } | **mac** { *source-mac-address*
| { **any** | **host** } *source-mac-address* } *source-mac-address-mask* { *destination-mac-address* |
{ **any** | **host** } *destination-mac-address* } *destination-mac-address-mask* }
**no monitor capture** *capture-name* **match**

## Syntax Description

| | |
|---|---|
| *epc-capture-name* | Name of the capture. |
| **any** | Specifies all packets. |
| **ipv4** | Specifies IPv4 packets. |
| **ipv6** | Specifies IPv6 packets. |
| *source-prefix/length* | The network prefix and length of the IPv4 or IPv6 source address. |
| **any** | Specifies network prefix of any source IPv4 or IPv6 address. |
| **host** | Specifies the source host. |
| *source-ip-address* | Source IPv4 or IPv6 address. |
| *destination-prefix/length* | Destination IPv4 or IPv6 address. |
| **any** | Specifies the network prefix and length of any IPv4 or IPv6 destination address. |
| **host** | Specifies the destination host. |
| *destination-ip-address* | Destination IPv4 or IPv6 address. |
| **protocol** | Specifies the protocol. |
| **tcp** | Specifies the TCP protocol. |
| **udp** | Specifies the UDP protocol. |
| **eq** | (Optional) Specifies that only packets with a port number that is equal to the port number associated with the IP address are matched. |

| | |
|---|---|
| **gt** | (Optional) Specifies that only packets with a port number that is greater than the port number associated with the IP address are matched. |
| **lt** | (Optional) Specifies that only packets with a port number that is lower than the port number associated with the IP address are matched. |
| **neq** | (Optional) Specifies that only packets with a port number that is not equal to the port number associated with the IP address are matched. |
| *port-number* | (Optional) The port number associated with the IP address. The range is from 0 to 65535. |
| **range** | (Optional) Specifies the range of port numbers. |
| *start-port-number* | (Optional) The start of the range of port numbers. The range is from 0 to 65535. |
| *end-port-number* | (Optional) The end of the range of port numbers. The range is from 0 to 65535. |
| **mac** | Specifies a Layer 2 packet. |
| *source-mac-address* | The source MAC address. |
| **any** | Specifies the network prefix of any source MAC address. |
| **host** | Specifies the MAC source host. |
| *source-mac-address-mask* | The source MAC address mask. |
| *destination-mac-address* | The destination MAC address. |
| **any** | Specifies the network prefix of any destination MAC address. |
| **host** | Specifies the MAC source host. |
| *destination-mac-address-mask* | The destination MAC address mask. |

### Command Modes

Privileged EXEC (#)

### Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 17.12.1 | This command was introduced. |

### Usage Guidelines

Use the **monitor capture** command to specify the core filter as a class map, access list, or explicit inline filter. Any filter has already specified before you enter the **monitor capture match** command is replaced.

## Examples

The following example shows how to set various explicit filters:

```
Device> enable
Device# monitor capture mycap match any
Device# monitor capture mycap match mac any any
Device# monitor capture mycap match ipv4 any any
Device# monitor capture mycap match ipv4 protocol udp 198.51.100.0/24 eq 20001 any
Device# end
```

The following example shows how to set a filter for MAC addresses:

```
Device> enable
Device# monitor capture match mycap mac 0030.9629.9f84 0000.0000.0000 0030.7524.9f84
0000.0000.0000
Device# end
```

The following example shows how to set a filter for IPv4 traffic:

```
Device> enable
Device# monitor capture match mycap ipv4 198.51.100.0/24 198.51.100.1 203.0.113.0/24
203.0.113.254
Device# end
```

# monitor capture start

To start the capture of packet data at a traffic trace point into a buffer, use the **monitor capture start** command in privileged EXEC mode.

**monitor capture** *epc-capture-name* **start**

## Syntax Description

| | |
|---|---|
| *epc-capture-name* | Name of the capture. |

## Command Default

Data packets are not captured into a buffer.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.12.1 | This command was introduced. |

## Usage Guidelines

Use the **monitor capture start** command to enable the packet data capture after the capture point is defined. To stop the capture of packet data, use the **monitor capture stop** command.

Ensure that system resources such as CPU and memory are available before starting a capture.

## Examples

The following example shows how to start capture buffer contents:

```
Device> enable
Device# monitor capture mycap start
Device# monitor capture mycap export tftp://10.1.88.9/mycap.pcap
Device# monitor capture mycap limit packets 100 duration 60
Device# monitor capture mycap start
Device# end
```

# monitor capture stop

To stop the capture of packet data at a traffic trace point, use the **monitor capture stop** command in privileged EXEC mode.

**monitor capture** *epc-capture-name* **stop**

## Syntax Description

| | |
|---|---|
| *epc-capture-name* | Name of the capture. |

## Command Default

The packet data capture is ongoing.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.12.1 | This command was introduced. |

## Usage Guidelines

Use the **monitor capture start** command to start the capture of packet data that you started by using the **monitor capture start** command. You can configure two types of capture buffers: linear and circular. When the linear buffer is full, data capture stops automatically. When the circular buffer is full, data capture starts from the beginning and the data is overwritten.

## Examples

The following example shows how to stop capture buffer contents:

```
Device> enable
Device# monitor capture mycap stop
Device# end
```

# mop enabled

To enable an interface to support the Maintenance Operation Protocol ( MOP), use the **mopenabled** 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

| Release | Modification |
|---|---|
| 10.0 | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Examples

The following example enables MOP for serial interface 0:

```
Router(config)# interface serial 0
Router(config-if)# mop enabled
```

## Related Commands

| Command | Description |
|---|---|
| **mop retransmit-timer** | Configures the length of time that the Cisco IOS software waits before sending boot requests again to a MOP server. |
| **mop retries** | Configures the number of times the Cisco IOS software will send boot requests again to a MOP server. |
| **mop sysid** | Enables an interface to send out periodic MOP system identification messages. |

# mop sysid

To enable an interface to send out periodic Maintenance Operation Protocol (MOP) system identification messages, use the **mopsysid** command in interface configuration mode. To disable MOP message support on an interface, use the **no** form of this command.

**mop sysid**
**no mop sysid**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Enabled

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 10.0 | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

You can still run MOP without having the background system ID messages sent. This command lets you use the MOP remote console, but does not generate messages used by the configurator.

## Examples

The following example enables serial interface 0 to send MOP system identification messages:

```
Router(config)# interface serial 0
Router(config-if)# mop sysid
```

## Related Commands

| Command | Description |
|---|---|
| **mop device-code** | Identifies the type of device sending MOP sysid messages and request program messages. |
| **mop enabled** | Enables an interface to support the MOP. |

# multicast

To configure mesh multicast mode, use the **multicast** command.

**multicast** { **in-only** | **in-out** | **regular** }

## Syntax Description

| | |
|---|---|
| **in-only** | Configures mesh multicast In Mode. |
| **in-out** | Configures mesh multicast In-Out Mode. |
| **regular** | Configures mesh multicast Regular Mode. |

## Command Default

in-out

## Command Modes

config-wireless-mesh-profile

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to configure the 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
```

# multicast vlan

To configure multicast on a single VLAN, use the **multicast vlan** command. To remove the multicast, use the **no** form of the command.

**multicast vlan** *vlan-id*
**no multicast vlan** *vlan-id*

## Syntax Description

| | |
|---|---|
| *vlan-id* | Specifies the VLAN ID. |

## Command Default

Disabled.

## Command Modes

Wireless policy configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to configure multicast:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy policy-test
Device(config-wireless-policy)# multicast vlan 12
```

# nac

To enable RADIUS Network Admission Control (NAC) support, use the **nac** command. To disable NAC support, use the **no** form of this command.

**nac** [ **ise** | **xwf** ]
**no** **nac**

## Syntax Description

| | |
|---|---|
| **ise** | Configures Radius NAC support (Identity Service Engine) |
| **xwf** | Configures Express Wi-Fi NAC support. |

## Command Default

NAC is disabled.

## Command Modes

Wireless policy configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to configure RADIUS NAC:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy default-policy-profile
Device(config-wireless-policy)# nac
```

# nas-id option2

To configure option 2 parameters for a NAS-ID, use the **nas-id option2** command.

**nas-id option2** {**sys-ip** | **sys-name** | **sys-mac** }

## Syntax Description

| | |
|---|---|
| **sys-ip** | System IP Address. |
| **sys-name** | System Name. |
| **sys-mac** | System MAC address. |

## Command Default

None

## Command Modes

config-aaa-policy

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to configure the system IP address for the NAS-ID:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless aaa policy profile-name
Device(config-aaa-policy)# nas-id option2 sys-ip
```

# network

To configure the network number in decimal notation, use the **network** command.

**network** *network-number* [*network-mask* | **secondary** ]

## Syntax Description

| | |
|---|---|
| *ipv4-address* | Network number in dotted-decimal notation. |
| *network-mask* | Network mask or prefix length. |
| **secondary** | Configure as secondary subnet. |

## Command Default

None

## Command Modes

dhcp-config

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to configure network number and the mask address:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ip dhcp pool name
Device(dhcp-config)# network 209.165.200.224 255.255.255.0
```

# nmsp cloud-services enable

To configure NMSP cloud services, use the **nmsp cloud-services enable** command.

**nmsp cloud-services enable**

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to enable NMSP cloud services:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# nmsp cloud-services enable
```

# nmsp cloud-services http-proxy

To configure the proxy for NMSP cloud server, use the **nmsp cloud-services http-proxy** command.

**nmsp cloud-services http-proxy** *proxy-server port*

## Syntax Description

| | |
|---|---|
| *proxy-server* | Enter the hostname or the IP address of the proxy server for NMSP cloud services. |
| *port* | Enter the proxy server port number for NMSP cloud services. |

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to configure the proxy for NMSP cloud server:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# nmsp cloud-services http-proxy host-name port-number
```

# nmsp cloud-services server token

To configure the NMSP cloud services server parameters, use the **nmsp cloud-services server token** command.

**nmsp cloud-services server token** *token*

## Syntax Description

| | |
|---|---|
| *token* | Authentication token for the NMSP cloud services. |

## Command Default

None

## Command Modes

config

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to configure the for the NMSP cloud services server parameters:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# nmsp cloud-services server token authentication-token
```

# nmsp cloud-services server url

To configure NMSP cloud services server URL, use the **nmsp cloud-services server url** command.

**nmsp cloud-services server url** *url*

## Syntax Description

| | |
|---|---|
| *url* | URL of the NMSP cloud services server. |

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to configure a URL for NMSP cloud services server:

```
Device(config)# nmps cloud-services server url http://www.example.com
```

# nmsp notification interval

To modify the Network Mobility Services Protocol (NMSP) notification interval value on the controller to address latency in the network, use the **nmsp notification interval** command in global configuration mode.

**nmsp notification interval** { **attachment** | **location** | **rssi** {**clients** | **rfid** | **rogues** {**ap** | **client** } } }

## Syntax Description

| | |
|---|---|
| **attachment** | Specifies the time used to aggregate attachment information. |
| **location** | Specifies the time used to aggregate location information. |
| **rssi** | Specifies the time used to aggregate RSSI information. |
| **clients** | Specifies the time interval for clients. |
| **rfid** | Specifies the time interval for rfid tags. |
| **rogues** | Specifies the time interval for rogue APs and rogue clients . |
| **ap** | Specifies the time used to aggregate rogue APs . |
| **client** | Specifies the time used to aggregate rogue clients. |

## Command Default

No default behavior or values.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to set the NMSP notification interval for the active RFID tags to 25 seconds:

```
Device# configure terminal
Device(config)# nmsp notification-interval rfid 25
Device(config)# end
```

This example shows how to modify NMSP notification intervals for device attachment (connecting to the network or disconnecting from the network) every 10 seconds:

```
Device# configure terminal
Device(config)# nmsp notification-interval attachment 10
Device(config)# end
```

This example shows how to configure NMSP notification intervals for location parameters (location change) every 20 seconds:

```
Device# configure terminal
Device(config)# nmsp notification-interval location 20
Device(config)# end
```

# nmsp strong-cipher

To enable the new ciphers, use the **nmsp strong-cipher** command in global configuration mode. To disable, use the **no** form of this command.

**nmsp strong-cipher**
**no nmsp strong-cipher**

## Syntax Description

This command has no arguments or keywords.

## Command Default

The new ciphers are not enabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.2(2)E | This command was introduced. |

## Usage Guidelines

The **nmsp strong-cipher** command enables strong ciphers for new Network Mobility Service Protocol (NMSP) connections.

**Note** The existing NMSP connections will use the default cipher.

## Examples

The following example shows how to enable a strong-cipher for NMSP:

```
Device> enable
Device> configure terminal
Device(config)# nmsp strong-cipher
```

## Related Commands

| Command | Description |
|---|---|
| **show nmsp status** | Displays the status of active NMSP connections. |

# 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to enable 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 for , use the **option** command in flow exporter configuration mode. To remove optional data parameters for a flow exporter, use the **no** form of this command.

**option** {**exporter-stats** | **interface-table** | **sampler-table**} [**timeout** *seconds*]
**no option** {**exporter-stats** | **interface-table** | **sampler-table**}

## Syntax Description

| | |
|---|---|
| **exporter-stats** | Configures the exporter statistics option for flow exporters. |
| **interface-table** | Configures the interface table option for flow exporters. |
| **sampler-table** | Configures the export sampler table option for flow exporters. |
| **timeout** *seconds* | (Optional) Configures the option resend time in seconds for flow exporters. The range is 1 to 86400. The default is 600. |

## Command Default

The timeout is 600 seconds. All other optional data parameters are not configured.

## Command Modes

Flow exporter configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

The **option exporter-stats** command causes the periodic sending of the exporter statistics, including the number of records, bytes, and packets sent. This command allows the collector to estimate packet loss for the export records it receives. The optional timeout alters the frequency at which the reports are sent.

The **option interface-table** command causes the periodic sending of an options table, which allows the collector to map the interface SNMP indexes provided in the flow records to interface names. The optional timeout can alter the frequency at which the reports are sent.

The **option sampler-table** command causes the periodic sending of an options table, which details the configuration of each sampler and allows the collector to map the sampler ID provided in any flow record to a configuration that it can use to scale up the flow statistics. The optional timeout can alter the frequency at which the reports are sent.

To return this command to its default settings, use the **no option** or **default option** flow exporter configuration command.

The following example shows how to enable the periodic sending of the sampler option table, which allows the collector to map the sampler ID to the sampler type and rate:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# option sampler-table
```

The following example shows how to enable the periodic sending of the exporter statistics, including the number of records, bytes, and packets sent:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# option exporter-stats
```

The following example shows how to enable the periodic sending of an options table, which allows the collector to map the interface SNMP indexes provided in the flow records to interface names:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# option interface-table
```

# packet-capture

To enable packet capture on the AP profile, use the **packet-capture** command.

**packet-capture** *profile-name*

## Command Default

None

## Command Modes

config-ap-profile

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to configure parameter map type and name:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# parameter-map type subscriber attribute-to-service parameter-map-name
```

# parameter-map type webauth

To configure the webauth parameter type for a specific parameter map or all the parameter maps, use the **parameter-map type webauth** command.

**parameter-map type webauth** { *parameter-map-name* | **global** }

## Syntax Description

| | |
|---|---|
| *parameter-map-name* | Name of the parameter map. The map name is limited to 99 characters. |
| **global** | Applies the configuration to all the parameter maps. |

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

## Examples

The following example shows how to configure the webauth parameter type for a parameter map named *parameter-map1*:

```
Device# configure terminal
Device(config)# parameter-map type webauth parameter-map1
```

# password encryption aes

To enable strong (AES) password encryption, use the **password encryption aes** command. To disable this feature, use the **no** form of this command.

**password encryption aes**

```
no password  encryption aes
```

## Syntax Description

| | |
|---|---|
| **password** | Configures the encryption password (key). |
| **encryption** | Encrypts system passwords. |
| **aes** | Enables stronger (AES) password encryption. |

## Command Default

None

## Command Modes

Global configuration mode.

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.12.2s | This command was introduced. |

### Example

The following example shows how to enable AES password encryption :

```
Device(config)#password encryption aes
```

# peer-blocking

To configure peer-to-peer blocking on a WLAN, use the **peer-blocking** command. To disable peer-to-peer blocking, use the **no** form of this command.

**peer-blocking** {**drop** | **forward-upstream**}
**no peer-blocking**

## Syntax Description

| | |
|---|---|
| **drop** | Specifies the device to discard the packets. |
| **forward-upstream** | Specifies the packets to be forwarded on the upstream VLAN. The device next in the hierarchy to the device decides what action to take regarding the packets.<br>**Note** The **forward-upstream** option is not supported for Flex local switching. Traffic is dropped even if this option is configured. Also, peer to peer blocking for local switching SSIDs are available only for the clients on the same AP. |

## Command Default

Peer blocking is disabled.

## Command Modes

WLAN configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

This example shows how to enable the drop and forward-upstream options for peer-to-peer blocking:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1

Device(config-wlan)# peer-blocking  drop
Device(config-wlan)# peer-blocking forward-upstream
```

This example shows how to disable the drop and forward-upstream options for peer-to-peer blocking:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1

Device(config-wlan)# no peer-blocking  drop
Device(config-wlan)# no peer-blocking forward-upstream
```

# policy

To configure media stream admission policy, use the **policy** command.

**policy** {**admit** | **deny**}

## Syntax Description

| | |
|---|---|
| **admit** | Allows traffic for a media stream group. |
| **deny** | Denies traffic for a media stream group. |

## Command Default

None

## Command Modes

media-stream

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to allow traffic for a media stream group:

```
Device # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless media-stream group ms-group 224.0.0.0 224.0.0.223
Device(media-stream)# policy admit
```

# police

To define a policer for classified traffic, use the **police** command in policy-map class configuration mode. Use the **no** form of this command to remove an existing policer.

**police** *rate-bps* *burst-byte* [**conform-action transmit**]
**no police rate-bps** *burst-byte* [**conform-action transmit**]

## Syntax Description

| | |
|---|---|
| *rate-bps* | Specify the average traffic rate in bits per second (b/s). The range is 1000000 to 1000000000. |
| *burst-byte* | Specify the normal burst size in bytes. The range is 8000 to 1000000. |
| **conform-action transmit** | (Optional) When less than the specified rate, specify that the switch transmits the packet. |

## Command Default

No policers are defined.

## Command Modes

Policy-map class configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

A policer defines a maximum permissible rate of transmission, a maximum burst size for transmissions, and an action to take if either maximum is exceeded.

When configuring hierarchical policy maps, you can only use the **police** policy-map command in a secondary interface-level policy map.

The port ASIC device, which controls more than one physical port, supports 256 policers on the switch (255 user-configurable policers plus 1 policer reserved for internal use). The maximum number of configurable policers supported per port is 63. Policers are allocated on demand by the software and are constrained by the hardware and ASIC boundaries. You cannot reserve policers per port. There is no guarantee that a port will be assigned to any policer.

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

## Examples

This example shows how to configure a policer that transmits packets if traffic is less than 1 Mb/s average rate with a burst size of 20 KB. There is no packet modification.

```
Device(config)# class-map class1
Device(config-cmap)# exit
Device(config)# policy-map policy1
Device(config-pmap)# class class1
Device(config-pmap-c)# police 1000000 20000 conform-action transmit
Device(config-pmap-c)# exit
```

This example shows how to configure a policer that transmits packets if traffic is less than 1 Mb/s average rate with a burst size of 20 KB. There is no packet modification. This example uses an abbreviated syntax:

```
Device(config)# class-map class1
Device(config-cmap)# exit
Device(config)# policy-map policy1
Device(config-pmap)# class class1
Device(config-pmap-c)# police 1m 20000 conform-action transmit
Device(config-pmap-c)# exit
```

This example shows how to configure a policer, which marks down the DSCP values with the values defined in policed-DSCP map and sends the packet:

```
Device(config)# policy-map policy2
Device(config-pmap)# class class2
Device(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
Device(config-pmap-c)# exit
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

# police cir

To set the policing of committed information rate, use the **police cir** command.

**police cir** *<target bit rate>*

## Syntax Description

| | |
|---|---|
| **police cir** | Polices committed information rate. |
| *8000-10000000000* | Sets the target bit rate at bits per second. The range is between 8000 and 10000000000. |

## Command Default

None

## Command Modes

Policy map class configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Amsterdam 17.2.1 | This command was introduced. |

### Example

This example shows how to set the committed information rate:

```
Device(config-pmap-c)#police cir 8000
```

# policy-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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

The AP will disconnect and rejoin after running this command.

### Example

The following example shows how to configure 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

After entering the **policy-map** command, you enter policy-map configuration mode, and these configuration commands are available:

- **class**—Defines the classification match criteria for the specified class map.
- **description**—Describes the policy map (up to 200 characters).
- **exit**—Exits policy-map configuration mode and returns you to global configuration mode.
- **no**—Removes a previously defined policy map.
- **sequence-interval**—Enables sequence number capability.

To return to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

Before configuring policies for classes whose match criteria are defined in a class map, use the **policy-map** command to specify the name of the policy map to be created, added to, or modified. Entering the **policy-map** command also enables the policy-map configuration mode in which you can configure or modify the class policies for that policy map.

You can configure class policies in a policy map only if the classes have match criteria defined for them. To configure the match criteria for a class, use the **class-map** global configuration and **match** class-map configuration commands. You define packet classification on a physical-port basis.

Only one policy map per ingress port is supported. You can apply the same policy map to multiple physical ports.

You can apply a nonhierarchical policy maps to physical ports. A nonhierarchical policy map is the same as the port-based policy maps in the device.

A hierarchical policy map has two levels in the format of a parent-child policy. The parent policy cannot be modified but the child policy (port-child policy) can be modified to suit the QoS configuration.

In VLAN-based QoS, a service policy is applied to an SVI interface.

**Note** Not all MQC QoS combinations are supported for wired ports. For information about these restrictions, see chapters "Restrictions for QoS on Wired Targets" in the QoS configuration guide.

## Examples

This example shows how to create a policy map called policy1. When attached to the ingress port, it matches all the incoming traffic defined in class1, sets the IP DSCP to 10, and polices the traffic at an average rate of 1 Mb/s and bursts at 20 KB. Traffic less than the profile is sent.

```
Device(config)# policy-map policy1
Device(config-pmap)# class class1
Device(config-pmap-c)# set dscp 10
Device(config-pmap-c)# police 1000000 20000 conform-action transmit
Device(config-pmap-c)# exit
```

This example show you how to configure hierarchical polices:

```
Device# configure terminal
Device(config)# class-map c1
Device(config-cmap)# exit

Device(config)# class-map c2
Device(config-cmap)# exit

Device(config)# policy-map child
Device(config-pmap)# class c1
Device(config-pmap-c)# priority level 1
Device(config-pmap-c)# police rate percent 20 conform-action transmit exceed action drop
Device(config-pmap-c-police)# exit
Device(config-pmap-c)# exit

Device(config-pmap)# class c2
Device(config-pmap-c)# bandwidth 20000
Device(config-pmap-c)# exit

Device(config-pmap)# class class-default
Device(config-pmap-c)# bandwidth 20000
Device(config-pmap-c)# exit
Device(config-pmap)# exit

Device(config)# policy-map parent
Device(config-pmap)# class class-default
Device(config-pmap-c)# shape average 1000000
Device(config-pmap-c)# service-policy child
Deviceconfig-pmap-c)# end
```

This example shows how to delete a policy map:

```
Device(config)# no policy-map policymap2
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

# policy-map

To create or modify a policy map that can be attached to multiple physical ports or switch virtual interfaces (SVIs) and to enter policy-map configuration mode, use the **policy-map** command in global configuration mode. Use the **no** form of this command to delete an existing policy map and to return to global configuration mode.

**policy-map** *policy-map-name*
**no** **policy-map** *policy-map-name*

## Syntax Description

| | |
|---|---|
| *policy-map-name* | Name of the policy map. |

## Command Default

No policy maps are defined.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

After entering the **policy-map** command, you enter policy-map configuration mode, and these configuration commands are available:

- **class**—Defines the classification match criteria for the specified class map.
- **description**—Describes the policy map (up to 200 characters).
- **exit**—Exits policy-map configuration mode and returns you to global configuration mode.
- **no**—Removes a previously defined policy map.
- **sequence-interval**—Enables sequence number capability.

To return to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

Before configuring policies for classes whose match criteria are defined in a class map, use the **policy-map** command to specify the name of the policy map to be created, added to, or modified. Entering the **policy-map** command also enables the policy-map configuration mode in which you can configure or modify the class policies for that policy map.

You can configure class policies in a policy map only if the classes have match criteria defined for them. To configure the match criteria for a class, use the **class-map** global configuration and **match** class-map configuration commands. You define packet classification on a physical-port basis.

Only one policy map per ingress port is supported. You can apply the same policy map to multiple physical ports.

You can apply a nonhierarchical policy maps to physical ports. A nonhierarchical policy map is the same as the port-based policy maps in the device.

A hierarchical policy map has two levels in the format of a parent-child policy. The parent policy cannot be modified but the child policy (port-child policy) can be modified to suit the QoS configuration.

In VLAN-based QoS, a service policy is applied to an SVI interface.

**Note** Not all MQC QoS combinations are supported for wired ports. For information about these restrictions, see chapters "Restrictions for QoS on Wired Targets" in the QoS configuration guide.

## Examples

This example shows how to create a policy map called policy1. When attached to the ingress port, it matches all the incoming traffic defined in class1, sets the IP DSCP to 10, and polices the traffic at an average rate of 1 Mb/s and bursts at 20 KB. Traffic less than the profile is sent.

```
Device(config)# policy-map policy1
Device(config-pmap)# class class1
Device(config-pmap-c)# set dscp 10
Device(config-pmap-c)# police 1000000 20000 conform-action transmit
Device(config-pmap-c)# exit
```

This example show you how to configure hierarchical polices:

```
Device# configure terminal
Device(config)# class-map c1
Device(config-cmap)# exit

Device(config)# class-map c2
Device(config-cmap)# exit

Device(config)# policy-map child
Device(config-pmap)# class c1
Device(config-pmap-c)# priority level 1
Device(config-pmap-c)# police rate percent 20 conform-action transmit exceed action drop
Device(config-pmap-c-police)# exit
Device(config-pmap-c)# exit

Device(config-pmap)# class c2
Device(config-pmap-c)# bandwidth 20000
Device(config-pmap-c)# exit

Device(config-pmap)# class class-default
Device(config-pmap-c)# bandwidth 20000
Device(config-pmap-c)# exit
Device(config-pmap)# exit

Device(config)# policy-map parent
Device(config-pmap)# class class-default
Device(config-pmap-c)# shape average 1000000
Device(config-pmap-c)# service-policy child
Deviceconfig-pmap-c)# end
```

This example shows how to delete a policy map:

```
Device(config)# no policy-map policymap2
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

# port

To configure the port number to use when configuring the custom application, use the **port** command.

**port** *port-no*

## Syntax Description

| | |
|---|---|
| *port-no* | Port number. |

## Command Default

None

## Command Modes

config-custom

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to configure the port number to use when configuring the custom application:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ip nbar custom custom-protocol http host host-string
Device(config-custom)# http host hostname
Device(config-custom)# port port-no
```

# priority priority-value

To configure media stream priority, use the **priority** *priority-value* command.

**priority** *priority-value*

## Syntax Description

| | |
|---|---|
| *priority-value* | Media stream priority value. Valid range is 1 to 8, with 1 being lowest priority and 8 being highest priority. |

## Command Default

None

## Command Modes

config-media-stream

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to set the media stream priority value to the highest, that is 8:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless media-stream group my-media-group 224.0.0.0 224.0.0.223
Device(config-media-stream)# priority 8
```

# 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

| | |
|---|---|
| **out** | Enable the egress expedite queue. |

## Command Default

The egress expedite queue is disabled.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## 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 shape** 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

| Command | Description |
|---|---|
| **show mls qos interface queueing** | Displays the queueing strategy (SRR, priority queueing), the weights corresponding to the queues, and the CoS-to-egress-queue map. |
| **srr-queue bandwidth shape** | Assigns the shaped weights and enables bandwidth shaping on the four egress queues mapped to a port. |
| **srr-queue bandwidth share** | Assigns the shared weights and enables bandwidth sharing on the four egress queues mapped to a port. |

# 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* [*Kb/s* [*burst -in-bytes*] ] ]
**no priority** [*Kb/s* [*burst -in-bytes*] | **level** *level value* [*Kb/s* [*burst -in-bytes*] ] | **percent** *percentage* [*Kb/s* [*burst -in-bytes*] ] ]

## Syntax Description

## Command Default

No priority is set.

## Command Modes

Policy-map class configuration (config-pmap-c)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## 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:

```
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-police)#exit
Device(config-pmap-c)#exit
Device(config-pmap)#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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## 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
```

# public-ip

To configure the NAT public IP address of the controller, use the **public-ip** command.

**public-ip** { *ipv4-address* | *ipv6-address* }

## Syntax Description

| | |
|---|---|
| *ipv4-address* | Sets IPv4 address. |
| *ipv6-address* | Sets IPv6 address. |

## Command Default

None

## Command Modes

Management Interface Configuration(config-mgmt-interface)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

## Usage Guidelines

### Example

The following example shows how to configure the NAT public IP address of the controller:

```
Device# configure terminal
Device(config)# wireless management interface Vlan1
Device(config-mgmt-interface)# public-ip 192.168.172.100
```

# qos 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

| | |
|---|---|
| *range-of-multiplier* | You can specify a value in the range of 100 to 1200. The default value is 100. |

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| | This command was introduced. |

## Usage Guidelines

**Note** 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.

# qos video

To configure over-the-air QoS class to video only, use the **qos video** command.

**qos video**

## Command Default

None

## Command Modes

config-media-stream

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to configure over-the-air QoS class to video only:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless media-stream group my-media-group 224.0.0.0 224.0.0.223
Device(config-media-stream)# qos video
```

# 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

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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

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 | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | 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)# 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.<br>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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## 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

| Command | Description |
|---|---|
| mls qos queue-set output buffers | Allocates buffers to a queue set. |
| mls qos queue-set output threshold | Configures the weighted tail-drop (WTD) thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue set. |

# radius server

To configure the RADIUS server, use the **radius server** command in global configuration mode.

**radius server** *server-name*

## Syntax Description

| | |
|---|---|
| *server-name* | RADIUS server name. |

## Command Default

None

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

None

The following example shows how to configure a radius server:

```
Device(config)# radius server ISE
```

# radius-server deadtime

To improve RADIUS response times when some servers might be unavailable, use the **radius-server deadtime** command to cause the unavailable servers to be skipped immediately. To set dead-time to the default value of 0, use the **no** form of this command.

**radius-server deadtime** *time-in-minutes*

**no radius-server deadtime**

## Syntax Description

| | |
|---|---|
| *time-in-minutes* | Length of time, in minutes, for which a RADIUS server is skipped over by transaction requests, up to a maximum of 1440 minutes (24 hours). |

## Command Default

Dead time is set to 0.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

## Usage Guidelines

Use this command to mark as "dead" any RADIUS servers that fail to respond to authentication requests, thus avoiding the wait for the request to time out before trying the next configured server. A RADIUS server marked as "dead" is skipped by additional requests for the duration of minutes or unless there are no servers not marked "dead."

### Example

The following example shows how to set deadtime for RADIUS servers that fail to respond to authentication requests:

```
Device(config)# radius-server deadtime 5
```

# radius-server attribute wireless accounting call-station-id

To configure call station identifier sent in the RADIUS accounting messages, use the **radius-server attribute wireless accounting call-station-id** command. To remove the call station identifier from the radius accounting messages, use the **no** form of the command.

**radius-server attribute wireless authentication call-station-id** { **ap-ethmac-only** | **ap-ethmac-ssid** | **ap-ethmac-ssid-flexprofilename** | **ap-ethmac-ssid-policytagname** | **ap-ethmac-ssid-sitetagname** | **ap-group-name** | **ap-label-address** | **ap-label-address-ssid** | **ap-location** | **ap-macaddress** | **ap-macaddress-ssid** | **ap-macaddress-ssid-flexprofilename** | **ap-macaddress-ssid-policytagname** | **ap-macaddress-ssid-sitetagname** | **ap-name** | **ap-name-ssid** | **flex-profile-name** | **ipaddress** | **macaddress** | **policy-tag-name** | **site-tag-name** | **vlan-id** }

## Syntax Description

| | |
|---|---|
| **ap-ethmac-only** | Sets the call station identifier type to be AP's radio MAC address. |
| **ap-ethmac-ssid** | Sets the call station identifier type AP's radio MAC address with SSID. |
| **ap-ethmac-ssid-flexprofilename** | Sets the call station identifier type AP's radio MAC address with SSID and flex profile name. |
| **ap-ethmac-ssid-policytagname** | Sets the call station identifier type AP's radio MAC address with SSID and policy tag name. |
| **ap-ethmac-ssid-sitetagname** | Sets the call station identifier type AP's radio MAC address with SSID and site tag name. |
| **ap-group-name** | Sets the call station identifier type to use the AP group name. |
| **ap-label-address** | Sets the call station identifier type to the AP's radio MAC address that is printed on the AP label. |
| **ap-label-address-ssid** | Sets the call station identifier type to the AP's radio MAC address and SSID that is printed on the AP label. |
| **ap-location** | Sets the call station identifier type to the AP location. |
| **ap-macaddress** | Sets the call station identifier type to the AP's radio MAC address. |
| **ap-macaddress-ssid** | Sets the call station identifier type to the AP's radio MAC address with SSID. |
| **ap-macaddress-ssid-flexprofilename** | Sets the call station identifier type to the AP's radio MAC address with SSID and flex profile name. |
| **ap-macaddress-ssid-policytagname** | Sets the call station identifier type to the AP's radio MAC address with SSID and policy tag name. |
| **ap-macaddress-ssid-sitetagname** | Sets the call station identifier type to the AP's radio MAC address with SSID and site tag name. |
| **ap-name** | Sets the call station identifier type to the AP name. |

| | |
|---|---|
| **ap-name-ssid** | Sets the call station identifier type to the AP name with SSID. |
| **flex-profile-name** | Sets the call station identifier type to the flex profile name. |
| **ipaddress** | Sets the call station identifier type to the IP address of the system. |
| **macaddress** | Sets the call station identifier type to the MAC address of the system. |
| **policy-tag-name** | Sets the call station identifier type to the policy tag name. |
| **site-tag-name** | Sets the call station identifier type to the site tag name. |
| **vlan-id** | Sets the call station identifier type to the system's VLAN ID. |

## Command Default

Call station identifier is not configured.

## Command Modes

Global Configuration(config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.12.1 | This command was introduced. |
| Cisco IOS XE Bengaluru 17.4.1 | This command was modified. The **policy-tag-name**, **flex-profile-name**, **ap-macaddress-ssid-flexprofilename**, **ap-macaddress-ssid-policytagname**, **ap-macaddress-ssid-sitetagname**, **ap-ethmac-ssid-flexprofilename**, **ap-ethmac-ssid-policytagname**, and **ap-ethmac-ssid-sitetagname** keywords were introduced. |

## Usage Guidelines

### Example

The following example shows how to configure a call station identifier sent in the RADIUS accounting messages:

```
Device(config)# radius-server attribute wireless accounting call-station-id site-tag-name
```

# radius-server attribute wireless authentication call-station-id

To configure call station identifier sent in the RADIUS authentication messages, use the **radius-server attribute wireless authentication call-station-id** command. To remove the call station identifier from the radius accounting messages, use the **no** form of the command.

**radius-server attribute wireless authentication call-station-id** { **ap-ethmac-only** | **ap-ethmac-ssid** | **ap-ethmac-ssid-flexprofilename** | **ap-ethmac-ssid-policytagname** | **ap-ethmac-ssid-sitetagname** | **ap-group-name** | **ap-label-address** | **ap-label-address-ssid** | **ap-location** | **ap-macaddress** | **ap-macaddress-ssid** | **ap-macaddress-ssid-flexprofilename** | **ap-macaddress-ssid-policytagname** | **ap-macaddress-ssid-sitetagname** | **ap-name** | **ap-name-ssid** | **flex-profile-name** | **ipaddress** | **macaddress** | **policy-tag-name** | **site-tag-name** | **vlan-id** }

## Syntax Description

| | |
|---|---|
| **ap-ethmac-only** | Sets the call station identifier type to be AP's radio MAC address. |
| **ap-ethmac-ssid** | Sets the call station identifier type AP's radio MAC address with SSID. |
| **ap-ethmac-ssid-flexprofilename** | Sets the call station identifier type AP's radio MAC address with SSID and flex profile name. |
| **ap-ethmac-ssid-policytagname** | Sets the call station identifier type AP's radio MAC address with SSID and policy tag name. |
| **ap-ethmac-ssid-sitetagname** | Sets the call station identifier type AP's radio MAC address with SSID and site tag name. |
| **ap-group-name** | Sets the call station identifier type to use the AP group name. |
| **ap-label-address** | Sets the call station identifier type to the AP's radio MAC address that is printed on the AP label. |
| **ap-label-address-ssid** | Sets the call station identifier type to the AP's radio MAC address and SSID that is printed on the AP label. |
| **ap-location** | Sets the call station identifier type to the AP location. |
| **ap-macaddress** | Sets the call station identifier type to the AP's radio MAC address. |
| **ap-macaddress-ssid** | Sets the call station identifier type to the AP's radio MAC address with SSID. |
| **ap-macaddress-ssid-flexprofilename** | Sets the call station identifier type to the AP's radio MAC address with SSID and flex profile name. |
| **ap-macaddress-ssid-policytagname** | Sets the call station identifier type to the AP's radio MAC address with SSID and policy tag name. |
| **ap-macaddress-ssid-sitetagname** | Sets the call station identifier type to the AP's radio MAC address with SSID and site tag name. |
| **ap-name** | Sets the call station identifier type to the AP name. |

| | |
|---|---|
| **ap-name-ssid** | Sets the call station identifier type to the AP name with SSID. |
| **flex-profile-name** | Sets the call station identifier type to the flex profile name. |
| **ipaddress** | Sets the call station identifier type to the IP address of the system. |
| **macaddress** | Sets the call station identifier type to the MAC address of the system. |
| **policy-tag-name** | Sets the call station identifier type to the policy tag name. |
| **site-tag-name** | Sets the call station identifier type to the site tag name. |
| **vlan-id** | Sets the call station identifier type to the system's VLAN ID. |

## Command Default

Call station identifier is not configured.

## Command Modes

Global Configuration(config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.12.1 | This command was introduced. |
| Cisco IOS XE Bengaluru 17.4.1 | This command was modified. The **policy-tag-name**, **flex-profile-name**, **ap-macaddress-ssid-flexprofilename**, **ap-macaddress-ssid-policytagname**, **ap-macaddress-ssid-sitetagname**, **ap-ethmac-ssid-flexprofilename**, **ap-ethmac-ssid-policytagname**, and **ap-ethmac-ssid-sitetagname** keywords were introduced. |

## Usage Guidelines

### Example

The following example shows how to configure a call station identifier sent in the RADIUS authentication messages:

```
Device(config)# radius-server attribute wireless authentication call-station-id site-tag-name
```

# range

To configure range from MAP to RAP bridge, use the **range** command.

**range** *range-in-feet*

## Syntax Description

| | |
|---|---|
| *range-in-feet* | Configure the range value in terms of feet. Valid range is from 150 feet to 132000 feet. |

## Command Default

1200

## Command Modes

config-wireless-mesh-profile

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to configure range from MAP to RAP bridge for a mesh AP profile:

```
Device # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device (config)# wireless profile mesh mesh-profile
Device (config-wireless-mesh-profile)# range 300
```

# 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 | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to configure an AVC reanchor classname:

```
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.

**redundancy revertive**

## Syntax Description

This command has no keywords or arguments.

## Command Default

None

## Command Modes

EoGRE domain configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.11.1 | This command was introduced. |

### 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

| | |
|---|---|
| **for-login** | To login, redirect to this URL. |
| **on-failure** | If login fails, redirect to this URL. |
| **on-success** | If login is sucessful, redirect to this URL. |
| *redirect-url-name* | Redirect URL name. |

## Command Default

None

## Command Modes

config-params-parameter-map

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to configure an redirect to an external IPv4 URL to login:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# parameter-map type webauth parameter-name
Device(config-params-parameter-map)# redirect for-login cisco.com
```

# redirect portal

To configure external IPv4 or IPv6 portal, use the **redirect portal** command.

**redirect portal** {**ipv4** | **ipv6** }*ip-addr*

## Syntax Description

| | |
|---|---|
| **ipv4** | IPv4 portal address |
| **ipv6** | IPv6 portal address |

## Command Default

None

## Command Modes

config-params-parameter-map

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to configure an external IPv4 portal address:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# parameter-map type webauth parameter-name
Device(config-params-parameter-map)# redirect portal ipv4 192.168.1.100
```

# remote-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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

### Example

This example shows how to map an RLAN policy profile to an RLAN profile:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless tag policy remote-lan-policy-tag
Device(config-policy-tag)# remote-lan rlan_profile_name policy rlan_policy_profile port-id
 2
Device(config-policy-tag)# end
```

# rf tag

To configure an RF tag to the AP, use the **rf tag**command.

**rf tag** *rf-tag-name*

## Syntax Description

| | |
|---|---|
| *rf-tag-name* | RF tag name. |

## Command Default

None

## Command Modes

config-ap-tag

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

The AP will disconnect and rejoin after running this command.

### Example

The following example shows how to configure an RF tag:

```
Device(config-ap-tag)# rf-tag rftag1
```

# rrc-evaluation

To configure Resource Reservation Control (RRC) reevaluation admission, use the **rrc-evaluation** command.

**rrc-evaluation** {**initial** | **periodic**}

## Syntax Description

| | |
|---|---|
| **initial** | Configures initial admission evaluation. |
| **periodic** | Configures periodic admission evaluation. |

## Command Default

None

## Command Modes

config-media-stream

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to configure the RRC reevaluation admission to initial admission evaluation.

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless media-stream group my-media-group 224.0.0.0 224.0.0.223
Device(config-media-stream)# rrc-evaluation initial
```

# security

To configure mesh security, use the **security** command.

**security** { **eap** | **psk** }

## Syntax Description

| | |
|---|---|
| **eap** | Configure mesh security EAP for Mesh AP. |
| **psk** | Configure mesh security PSK for Mesh AP |

## Command Default

EAP

## Command Modes

config-wireless-mesh-profile

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to configure mesh security with EAP protcol on an Mesh AP:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile mesh profile-name
Device(config-wireless-mesh-profile)# security eap
```

# security dot1x authentication-list

To configure security authentication list for IEEE 802.1x, use the **security dot1x authentication-list** *auth-list-name* command.

**security dot1x authentication-list** *auth-list-name*

## Syntax Description

| Parameter | Description |
|---|---|
| *auth-list-name* | Authentication list name. |

## Command Default

None

## Command Modes

config-wlan

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to configure security authentication list for IEEE 802.1x:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan-name
Device(config-wlan)# security dot1x authentication-list auth-list-realm
```

# security ft

To configure 802.11r fast transition parameters, use the **security ft** command. To configure fast transition **over the air**, use the **no security ft over-the-ds** command.

**security ft** [**over-the-ds** | **reassociation-timeout** *timeout-jn-seconds*]
**no security ft** [**over-the-ds** | **reassociation-timeout**]

## Syntax Description

| | |
|---|---|
| **over-the-ds** | (Optional) Specifies that the 802.11r fast transition occurs over a distributed system. The no form of the command with this parameter configures security ft over the air. |
| **reassociation-timeout** | (Optional) Configures the reassociation timeout interval. |
| *timeout-in-seconds* | (Optional) Specifies the reassociation timeout interval in seconds. The valid range is between 1 to 100. The default value is 20. |

## Command Default

The feature is disabled.

## Command Modes

WLAN configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

None

WLAN Security must be enabled.

### Example

The following example configures security FT configuration for an open WLAN:

```
Device#wlan test
Device(config-wlan)# client vlan 0140
Device(config-wlan)# no mobility anchor sticky
Device(config-wlan)# no security wpa
Device(config-wlan)# no security wpa akm dot1x
Device(config-wlan)# no security wpa wpa2
Device(config-wlan)# no security wpa wpa2 ciphers aes
Device(config-wlan)# security ft
Device(config-wlan)# shutdown
```

The following example shows a sample security FT on a WPA-enabled WLAN:

```
Device# wlan test
Device(config-wlan)# client vlan 0140
Device(config-wlan)# no security wpa akm dot1x
Device(config-wlan)# security wpa akm ft psk
Device(config-wlan)# security wpa akm psk set-key ascii 0 test-test
Device(config-wlan)# security ft
Device(config-wlan)# no shutdown
```

# security 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

| | |
|---|---|
| **glean** | Extracts addresses from the messages and installs them into the binding table without performing any verification. |
| **guard** | 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. |
| **inspect** | Validates messages for consistency and conformance; in particular, address ownership is enforced. Invalid messages are dropped. |

## Command Default

The default security level is guard.

## Command Modes

IPv6 snooping configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

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

| | |
|---|---|
| **association-comeback** | Configures the 802.11w association comeback time. |
| *association-comeback-time-seconds* | Association comeback interval in seconds. Time interval that an associated client must wait before the association is tried again after it is denied with a status code 30. The status code 30 message is "Association request rejected temporarily; Try again later.”<br>The range is from 1 through 20 seconds. |
| **mandatory** | Specifies that clients are required to negotiate 802.1w PMF protection on the WLAN. |
| **optional** | Specifies that the WLAN does not mandate 802.11w support on clients. Clients with no 802.11w capability can also join. |
| **saquery-retry-time** | Time interval identified before which the SA query response is expected. If the device does not get a response, another SA query is tried. |
| *saquery-retry-time-milliseconds* | The saquery retry time in milliseconds. The range is from 100 to 500 ms. The value must be specified in multiples of 100 milliseconds. |

## Command Default

PMF is disabled.

## Command Modes

WLAN configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

You must have WPA (Wi-Fi Protected Access) and AKM (Authentication Key Management) configured to use this feature. See Related Command section for more information on configuring the security parameters.

802.11w introduces an Integrity Group Temporal Key (IGTK) that is used to protect broadcast or multicast robust management frames. IGTK is a random value, assigned by the authenticator station (device) used to protect MAC management protocol data units (MMPDUs) from the source STA. The 802.11w IGTK key is derived using the four-way handshake and is used only on WLANs that are configured with WPA2 security at Layer 2.

This example shows how to enable the association comeback value at 15 seconds.

```
Device(config-wlan)# security pmf association-comeback 15
```

This example shows how to configure mandatory 802.11w MPF protection for clients on a WLAN:

```
Device(config-wlan)# security pmf mandatory
```

This example shows how to configure optional 802.11w MPF protection for clients on a WLAN:

```
Device(config-wlan)# security pmf optional
```

This example shows how to configure the saquery parameter:

```
Device(config-wlan)# security pmf saquery-retry-time 100
```

This example shows how to disable the PMF feature:

```
Device(config-wlan)# no security pmf
```

# security static-wep-key

To configure static WEP keys on a WLAN, use the **security static-wep-key** command.

**security static-wep-key** {**authentication** {**open** | **sharedkey** } | **encryption** {**104** | **40** } {**ascii** | **hex** | {**0** | **8** }*wep-key* | **wep-index** }}

## Syntax Description

| | |
|---|---|
| **open** | Open system authentication. |
| **sharedkey** | Shared key authentication. |
| **0** | Specifies an UNENCRYPTED password is used. |
| **8** | Specifies an AES encrypted password is used. |
| *wep-key* | Enter the name of the WEP key. |

## Command Default

None

## Command Modes

config-wlan

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to authenticate 802.11 using shared key:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan profile-name wlan-id
Device(config-wlan)# security static-wep-key authentication sharedkey
```

# security web-auth

To change the status of web authentication used on a WLAN, use the **security web-auth** command. To disable web authentication on a WLAN, use the **no** form of the command.

**security web-auth** [**authentication-list** *authentication-list-name* | **on-macfilter-failure** | **parameter-map** *parameter-map-name*]
**no security web-auth** [**authentication-list** [**authentication-list-name**] | **on-macfilter-failure** | **parameter-map** [**parameter-name**]]

## Syntax Description

| | |
|---|---|
| **authentication-list** *authentication-list-name* | Sets the authentication list for IEEE 802.1x. |
| **on-macfilter-failure** | Enables web authentication on MAC failure. |
| **parameter-map** *parameter-map-name* | Configures the parameter map. |

## Command Default

Web authentication is disabled.

## Command Modes

WLAN configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

### Examples

The following example shows how to configure the authentication-list web authentication on a WLAN:

```
Device(config-wlan)# security web-auth authentication-list test
```

# security wpa akm

To configure authentication key management using Cisco Centralized Key Management (CCKM), use the **security wpa akm** command. To disable the authentication key management for Cisco Centralized Key Management, use the **no** form of the command.

**security wpa** [ **akm** { **cckm** | **dot1x** | **ft** | **pmf** | **psk** } | **wpa1** [ **ciphers** { **aes** | **tkip** } ] | **wpa2** [ **ciphers** { **aes** } ] ]
**no security wpa** [ **akm** { **cckm** | **dot1x** | **ft** | **pmf** | **psk** } | **wpa1** [ **ciphers** { **aes** | **tkip** } ] | **wpa2** [ **ciphers** { **aes** } ] ]

## Syntax Description

| | |
|---|---|
| **akm** | Configures the Authentication Key Management (AKM) parameters. |
| **aes** | Configures AES (Advanced Encryption Standard) encryption support. |
| **cckm** | Configures Cisco Centralized Key Management support. |
| **ciphers** | Configures WPA ciphers. |
| **dot1x** | Configures 802.1x support. |
| **ft** | Configures fast transition using 802.11r. |
| **pmf** | Configures 802.11w management frame protection. |
| **psk** | Configures 802.11r fast transition pre-shared key (PSK) support. |
| **tkip** | Configures Temporal Key Integrity Protocol (TKIP) encryption support. |
| **wpa2** | Configures Wi-Fi Protected Access 2 ( WPA2) support. |

## Command Default

By default Wi-Fi Protected Access2, 802.1x are enabled. WPA2, PSK, CCKM, FT dot1x, FT PSK, PMF dot1x, PMF PSK, FT Support are disabled. The FT Reassociation timeout is set to 20 seconds, PMF SA Query time is set to 200.

## Command Modes

WLAN Configuration (config-wlan)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

### Example

The following example shows how to configure CCKM on the WLAN.

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
Device(config)# wlan wlan1
Device(config-wlan)#security wpa akm cckm
```

# service-policy

To configure the quality of service (QoS) service policy, use the **service-policy** command. To disable a QoS policy, use the **no** form of this command.

**service-policy** { **client** | **input** | **output** } *policy-name*
**no** { **client** | **input** | **output** } *policy-name*

## Syntax Description

| | |
|---|---|
| **client** | Assigns a policy map to all clients in the WLAN. |
| **input** | Assigns an input policy map. |
| **output** | Assigns an output policy map. |
| *policy-name* | The policy map name. |

## Command Default

None

## Command Modes

Wireless policy configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Examples

This example shows how to configure the input service policy:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy default-policy-profile
Device(config-wireless-policy)# service-policy input test1
```

# service-policy qos

To configure a QoS service policy, use the **service-policy qos** command.

**service-policy qos** {**input** | **output**}*policy-name*

## Syntax Description

| | |
|---|---|
| **input** | Input QoS policy. |
| **output** | Output QoS policy. |
| *policy-name* | Policy name. |

## Command Default

None

## Command Modes

config-service-template

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to configure an output QoS policy:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# service-template fabric-profile-name
Device(config-service-template)# service-policy qos output policy-name
```

# service-template

To configure service template, use the **service-template** command.

**service-template** *service-template-name* {**access-group** *acl_list* | **vlan** *vlan_id* | **absolute-timer** *seconds* | **service-policy qos** {**input** | **output**} }

## Syntax Description

| | |
|---|---|
| *service-template-name* | Name of the service template. |
| *acl_list* | Access list name to be applied. |
| *vlan_id* | VLAN ID. The VLAN ID value ranges from 1 to 4094. |
| *seconds* | Session timeout value for service template. The session timeout value ranges from 1 to 65535 seconds. |
| **service-policy qos** {**input** \| **output** | QoS policies for client. |

## Command Default

None

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

None

The following example shows how to configure service template:

```
Device#configure terminal
Device(config)#service-template cisco-phone-template
Device(config-service-template)#access-group foo-acl
Device(config-service-template)#vlan 100
Device(config-service-template)#service-policy qos input foo-qos
Device(config-service-template)#end
```

# service timestamps

To configure the system to time-stamp debugging or logging messages, use the**service timestamps** command in global configuration commands. Use the **no** form of this command to disable this service.

**service timestamps debug log** {**datetime** | **uptime***localtimemsecshow-timezoneyear*}
**no service timestamps debuglog**

## Syntax Description

| | |
|---|---|
| **debug** | Debug as the timestamp message type. |
| **log** | Log as the timestamp message type. |
| **datetime** | **datetime** |
| **uptime** | (Optional) Time stamp with time since the system was rebooted. |
| **localtime** | (Optional) Time stamp relative to the local time zone. |
| **msec** | (Optional) Include milliseconds in the date and time stamp. |
| **show-timezone** | (Optional) Include the time zone name in the time stamp. |
| **year** | (Optional) Include year in timestamp. |

## Command Default

No time-stamping.

If **service timestamps** is specified with no arguments or keywords, default is **service timestamps debug uptime**.

The default for **service timestamps debugdatetime** is to format the time in UTC, with no milliseconds and no time zone name.

The command **no service timestamps** by itself disables time stamps for both debug and log messages.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Amsterdam 17.1.1s | This command was introduced in a release earlier than Cisco IOS XE Amsterdam 17.1.1s. |

## Usage Guidelines

Time stamps can be added to either debugging or logging messages independently. The uptime form of the command adds time stamps in the format HHHH:MM:SS, indicating the time since the system was rebooted. The datetime form of the command adds time stamps in the format MMM DD HH:MM:SS, indicating the date and time according to the system clock. If the system clock has not been set, the date and time are preceded by an asterisk (*) to indicate that the date and time are probably not correct.

### Example

The following example enables time stamps on debugging messages, showing the time since reboot:

```
Device(config)# service timestamps debug uptime
```

The following example enables time stamps on logging messages, showing the current time and date relative to the local time zone, with the time zone name included:

```
Device(config)# service timestamps log datetime localtime show-timezone
```

# session-timeout

To configure session timeout for clients associated to a WLAN, use the **session-timeout** command. To restore the default value, use the **no** form of this command.

**session-timeout** **seconds**
**no** **session-timeout**

## Syntax Description

| | |
|---|---|
| *seconds* | Timeout or session duration in seconds. The range is from 300 to 86400. The default value is 1800.<br>Configuring 86400 is equivalent to max timeout. And value 0 is not recommended. |

## Command Default

None

## Command Modes

WLAN configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to configure a session timeout to 3600 seconds:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#wireless profile policy policy1
Device(config-wireless-policy)#session-timeout 3600
```

# set

To classify IP traffic by setting a Differentiated Services Code Point (DSCP) or an IP-precedence value in the packet, use the **set** command in policy-map class configuration mode. Use the **no** form of this command to remove traffic classification.

**set**
**cos** | **dscp** | **precedence** | **ip** | **qos-group** | **wlan**
**set cos**
{*cos-value* } | {**cos** | **dscp** | **precedence** | **qos-group** | **wlan**} [**table** *table-map-name*]
**set dscp**
{*dscp-value* } | {**cos** | **dscp** | **precedence** | **qos-group** | **wlan**} [**table** *table-map-name*]
**set ip** {**dscp** | **precedence**}
**set precedence** {*precedence-value* } | {**cos** | **dscp** | **precedence** | **qos-group**} [**table** *table-map-name*]
**set qos-group**
{*qos-group-value* | **dscp** [**table** *table-map-name*] | **precedence** [**table** *table-map-name*]}
**set wlan user-priority**
*user-priority-value* | **costable** *table-map-name* | **dscptable** *table-map-name* | **qos-grouptable** *table-map-name* | **wlantable** *table-map-name*

## Syntax Description

**cos**

Sets the Layer 2 class of service (CoS) value or user priority of an outgoing packet. You can specify these values:

- *cos-value*—CoS value from 0 to 7. You also can enter a mnemonic name for a commonly used value.
- Specify a packet-marking category to set the CoS value of the packet. If you also configure a table map for mapping and converting packet-marking values, this establishes the "map from" packet-marking category. Packet-marking category keywords:
  - **cos**—Sets a value from the CoS value or user priority.
  - **dscp**—Sets a value from packet differentiated services code point (DSCP).
  - **precedence**—Sets a value from packet precedence.
  - **qos-group**—Sets a value from the QoS group.
  - **wlan**—Sets the WLAN user priority values.
- (Optional)**table** *table-map-name*—Indicates that the values set in a specified table map are used to set the CoS value. Enter the name of the table map used to specify the CoS value. The table map name can be a maximum of 64 alphanumeric characters.

  If you specify a packet-marking category but do not specify the table map, the default action is to copy the value associated with the packet-marking category as the CoS value. For example, if you enter the **set cos precedence** command, the precedence (packet-marking category) value is copied and used as the CoS value.

| | |
|---|---|
| **dscp** | Sets the differentiated services code point (DSCP) value to mark IP(v4) and IPv6 packets. You can specify these values:<br>• *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.<br>• 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:<br>  • **cos**—Sets a value from the CoS value or user priority.<br>  • **dscp**—Sets a value from packet differentiated services code point (DSCP).<br>  • **precedence**—Sets a value from packet precedence.<br>  • **qos-group**—Sets a value from the QoS group.<br>  • **wlan**—Sets a value from WLAN.<br>• (Optional)**table** *table-map-name*—Indicates that the values set in a specified table map will be used to set the DSCP value. Enter the name of the table map used to specify the DSCP value. The table map name can be a maximum of 64 alphanumeric characters.<br>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:<br>• **dscp**—Specify an IP DSCP value from 0 to 63 or a packet marking category.<br>• **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:<br>• *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.<br>• Specify a packet marking category to set the precedence value of the packet.<br>  • **cos**—Sets a value from the CoS or user priority.<br>  • **dscp**—Sets a value from packet differentiated services code point (DSCP).<br>  • **precedence**—Sets a value from packet precedence.<br>  • **qos-group**—Sets a value from the QoS group.<br>• (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.<br>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.<br>• *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.<br>• **dscp**—Sets the original DSCP field value of the packet as the QoS group value.<br>• **precedence**—Sets the original precedence field value of the packet as the QoS group value.<br>• (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.<br>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:<br>• *wlan-user-priority*—Sets a WLAN user priority to the classified traffic. The range is 0 to 7.<br>• **cos**—Sets the Layer 2 CoS field value as the WLAN user priority.<br>• **dscp**—Sets the DSCP field value as the WLAN user priority.<br>• **precedence**—Sets the precedence field value as the WLAN user priority.<br>• **wlan**—Sets the WLAN user priority field value as the WLAN user priority.<br>• (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.<br>If you specify a packet-marking category but do not specify the table map, the default action is to copy the value associated with the packet-marking category as the WLAN user priority. For example, if you enter the **set wlan user-priority cos** command, the cos value (packet-marking category) is copied and used as the WLAN user priority. |

## Command Default

No traffic classification is defined.

## Command Modes

Policy-map class configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was intro |
| | The **cos**, **dscp**, **qos-grou** |

## 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

| | |
|---|---|
| **detail** | (Optional) Specifies the wireless CAPWAP HA details. |
| **event** | (Optional) Specifies the wireless CAPWAP HA events. |
| **dump** | (Optional) Specifies the wireless CAPWAP HA output. |
| **filter** *mac* | Specifies the MAC address. |
| *switch switch number* | Specifies the switch number. |
| **none** | (Optional) Specifies the no filter option. |
| **switch** *switch* | (Optional) Specifies the device number. |
| *filter name* | Trace adapted flag filter name. |
| *filter_value* | (Optional) Value of the filter. |
| **switch** *switch* | (Optional) Specifies the device number. |
| **filtered** | Specifies the filtered traces messages. |
| *switch* | Specifies the switch number. |
| **level** | Specifies the trace level. |
| **default** | Specifies the unset trace level value. |
| *trace_level* | Specifies the trace level. |
| **switch** *switch* | (Optional) Specifies the device number. |

## Command Default

None

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

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 in the , 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*}}

## Syntax Description

| | |
|---|---|
| **event** | (Optional) Specifies the wireless mobility high availability events. |
| **detail** | (Optional) Specifies the wireless mobility high availability details. |
| **dump** | (Optional) Specifies the wireless mobility high availability output. |
| **filter** | Specifies to trace adapted flag filter. |
| **mac** | Specifies the MAC address. |
| *WORD switch* | Specifies the switch. |
| *switch number* | Specifies the switch number. The value ranges from one to four. |
| **none** | Specifies no trace adapted flag filter. |
| **switch** *switch* | (Optional) Specifies the device number. |
| *filter_name* | Trace adapted flag filter name. |
| *filter_value* | Trace adapted flag filter value. |
| **switch** *switch* | Specifies the device number. |
| **level** | Specifies the trace level value. |
| **default** | Specifies the un-set trace level value. |
| *trace_level* | Specifies the trace level value. |
| **switch** *switch* | Specifies the device number. |
| **filtered** | Specifies the filtered trace messages. |
| *switch* | Specifies the switch. |

## Command Default

None

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

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 10:38:35.349 UTC 2 8135] Invalid sysIp: Skip plumbing MC-MA
tunnels.
[08/27/13 10:38:54.393 UTC 3 8135] Mobility version mismatch, v10 received,
 or m
sglen 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

| | |
|---|---|
| **event** | (Optional) Specifies trace QoS wireless AP event. |
| **event** *mac* | Specifies the MAC address of the AP. |
| **event** *none* | Specifies no MAC address value. |
| **error** | (Optional) Specifies trace QoS wireless AP errors. |
| **error** *mac* | Specifies the MAC address of the AP. |
| **error** *none* | Specifies no value. |
| **filter** | Specifies the trace adapted flag filter. |
| **filter** *mac* | Specifies the MAC address of the AP. |
| **filter** *none* | Specifies no value. |
| **switch** *switch* | Specifies the switch number. |
| *filter_name* | (Optional) Specifies the switch filter name. |
| *filter_value* | (Optional) Specifies the switch filter value. Value is one. |
| **switch** *switch* | (Optional) Specifies the switch number. Value is one. |
| **level** | Specifies the trace level. |
| **default** | Specifies the trace QoS wireless AP default. |
| *trace_level* | Trace level. |
| **switch** *switch* | (Optional) Specifies the switch number. Value is one. |

## Command Default

None

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to trace wireless QoS high availability:

```
Device# set trace QOS ap ha
```

# sgt-tag

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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to configure an 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
```

# site-tag

To map a site tag to the AP, use the **site-tag**command.

**site-tag** *site-tag-name*

## Syntax Description

| | |
|---|---|
| *site-tag-name* | Name of the site tag. |

## Command Default

None

## Command Modes

config-ap-tag

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

The AP will disconnect and rejoin after running this command.

### Example

The following example shows how to configure a site tag:

```
Device(config-ap-tag)# site-tag sitetag1
```

# snmp-server enable traps wireless

To enable wireless notifications for a host, use the **snmp-server enable traps wireless** command.

**snmp-server enable traps wireless** [ **AP** | **bsnMobileStation** | **MESH** | **bsnAutoRF** | **rogue** | **wireless_mobility** | **RRM** | **bsnGeneral** ]

## Syntax Description

| | |
|---|---|
| **AP** | Enables wireless SNMP traps for APs |
| **bsnMobileStation** | Enables wireless client traps |
| **MESH** | Enables wireless mesh traps |
| **bsnAutoRF** | Enables wireless RF related traps |
| **rogue** | Enables traps for wireless rogue |
| **wireless_mobility** | Enables traps for wireless mobility |
| **RRM** | Enables traps for wireless RRM |
| **bsnGeneral** | Enables general controller traps |

## Command Default

None

## Command Modes

Global Configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Bengaluru 17.4.1 | This command was introduced. |

## Examples

The following example shows how to enable wireless notifications for a host:

```
Device# snmp-server enable traps wireless MESH
```

# snmp-server group

To configure a new Simple Network Management Protocol (SNMP) group, use the **snmp-server group** command in global configuration mode. To remove a specified SNMP group, use the **no** form of this command.

**snmp-server group** *group-name* {**v1** | **v2c** | **v3** } [**access** [**ipv6** *named-access-list*] [*acl-numberacl-name*]] [**context** *context-name*] [**notify** *notify-view*] [**read** *read-view*] [**write** *write-view*]
**no snmp-server group** *group-name* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**context** *context-name*]

## Syntax Description

| | |
|---|---|
| *group-name* | Name of the group. |
| **v1** | Specifies that the group is using the SNMPv1 security model. SNMPv1 is the least secure of the possible SNMP security models. |
| **v2c** | Specifies that the group is using the SNMPv2c security model.<br>The SNMPv2c security model allows informs to be transmitted and supports 64-character strings. |
| **v3** | Specifies that the group is using the SNMPv3 security model.<br>SMNPv3 is the most secure of the supported security models. It allows you to explicitly configure authentication characteristics. |
| **context** | (Optional) Specifies the SNMP context to associate with this SNMP group and its views. |
| *context-name* | (Optional) Context name. |
| **read** | (Optional) Specifies a read view for the SNMP group. This view enables you to view only the contents of the agent. |
| *read-view* | (Optional) String of a maximum of 64 characters that is the name of the view.<br>The default is that the read-view is assumed to be every object belonging to the Internet object identifier (OID) space (1.3.6.1), unless the **read** option is used to override this state. |
| **write** | (Optional) Specifies a write view for the SNMP group. This view enables you to enter data and configure the contents of the agent. |
| *write-view* | (Optional) String of a maximum of 64 characters that is the name of the view.<br>The default is that nothing is defined for the write view (that is, the null OID). You must configure write access. |
| **notify** | (Optional) Specifies a notify view for the SNMP group. This view enables you to specify a notify, inform, or trap. |

| | |
|---|---|
| *notify-view* | (Optional) String of a maximum of 64 characters that is the name of the view.<br>By default, nothing is defined for the notify view (that is, the null OID) until the **snmp-server host** command is configured. If a view is specified in the **snmp-server group** command, any notifications in that view that are generated will be sent to all users associated with the group (provided a SNMP server host configuration exists for the user).<br>Cisco recommends that you let the software autogenerate the notify view. See the “Configuring Notify Views” section in this document. |
| **access** | (Optional) Specifies a standard access control list (ACL) to associate with the group. |
| **ipv6** | (Optional) Specifies an IPv6 named access list. If both IPv6 and IPv4 access lists are indicated, the IPv6 named access list must appear first in the list. |
| *named-access-list* | (Optional) Name of the IPv6 access list. |
| *acl-number* | (Optional) The *acl-number*argument is an integer from 1 to 99 that identifies a previously configured standard access list. |
| *acl-name* | (Optional) The *acl-name* argument is a string of a maximum of 64 characters that is the name of a previously configured standard access list. |

## Command Default

No SNMP server groups are configured.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Amsterdam 17.1.1s | This command was introduced in a release earlier than Cisco IOS XE Amsterdam 17.1.1s. |

## Usage Guidelines

When a community string is configured internally, two groups with the name public are autogenerated, one for the v1 security model and the other for the v2c security model. Similarly, deleting a community string will delete a v1 group with the name public and a v2c group with the name public.

No default values exist for authentication or privacy algorithms when you configure the **snmp-server group** command. Also, no default passwords exist. For information about specifying a Message Digest 5 (MD5) password, see the documentation of the **snmp-server user** command.

### Configuring Notify Views

The notify-view option is available for two reasons:

- If a group has a notify view that is set using SNMP, you may need to change the notify view.
- The **snmp-server host** command may have been configured before the **snmp-server group** command. In this case, you must either reconfigure the **snmp-server host** command, or specify the appropriate notify view.

Specifying a notify view when configuring an SNMP group is not recommended, for the following reasons:

- The **snmp-server host** command autogenerates a notify view for the user, and then adds it to the group associated with that user.

- Modifying the group’s notify view will affect all users associated with that group.

Instead of specifying the notify view for a group as part of the **snmp-server group** command, use the following commands in the order specified:

1. **snmp-server user** --Configures an SNMP user.
2. **snmp-server group** --Configures an SNMP group, without adding a notify view .
3. **snmp-server host** --Autogenerates the notify view by specifying the recipient of a trap operation.

**SNMP Contexts**

SNMP contexts provide VPN users with a secure way of accessing MIB data. When a VPN is associated with a context, that VPN’s specific MIB data exists in that context. Associating a VPN with a context enables service providers to manage networks with multiple VPNs. Creating and associating a context with a VPN enables a provider to prevent the users of one VPN from accessing information about users of other VPNs on the same networking device.

Use this command with the **context** *context-name* keyword and argument to associate a read, write, or notify SNMP view with an SNMP context.

### Create an SNMP Group

The following example shows how to create the SNMP server group “public,” allowing read-only access for all objects to members of the standard named access list “lmnop”:

```
Device(config)# snmp-server group public v2c access lmnop
```

### Remove an SNMP Server Group

The following example shows how to remove the SNMP server group “public” from the configuration:

```
Device(config)# no snmp-server group public v2c
```

### Associate an SNMP Server Group with Specified Views

The following example shows SNMP context “A” associated with the views in SNMPv2c group “GROUP1”:

```
Device(config)# snmp-server context A
Device(config)# snmp mib community commA
Device(config)# snmp mib community-map commA context A target-list commAVpn
Device(config)# snmp-server group GROUP1 v2c context A read viewA write viewA notify viewB
```

# snmp-server subagent cache

To prevent CPU spikes in the controller during Simple Network Management Protocol (SNMP) polling, use the **snmp-server subagent cache** command. To disable the subagent cache, use the **no** form of this command.

**snmp-server subagent cache** [ **timeout** *seconds* ]

**snmp-server subagent cache** [ **timeout** *seconds* ]

## Syntax Description

| | |
|---|---|
| **timeout** | Specifies the subagent cache timeout. |
| *seconds* | The server timeout value, in seconds. The valid values range from 1 to 100, with a default of 60. |

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Dublin 17.11.1 | This command was introduced. |

## Usage Guidelines

Use this command to prevent CPU spikes in the controller by clearing the cache at regular intervals.

## Examples

The following example shows how to prevent CPU spikes in the controller during SNMP polling:

```
Device# configure terminal
Device(config)# snmp-server subagent cache
```

# ssid broadcast persistent

To enable the SSID broadcast mode, use the **ssid broadcast persistent** command. Use the **no** form of the command to disable the feature.

**ssid broadcast persistent**

**no ssid broadcast persistent**

## Syntax Description

This command has no keywords or arguments.

## Command Default

None

## Command Modes

AP profile configuration (config-ap-profile)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.12.1 | This command was introduced. |

## Usage Guidelines

Enabling or disabling this feature causes the AP to re-join.

## Examples

The following example shows how to enable the SSID broadcast mode:

```
Device# configure terminal
Device(config)# ap profile ap-profile-name
Device(config-ap-profile)# ssid broadcast persistent
```

# 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

### 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
```

# stopbits

To configure the stop bits for the console port, use the **stopbits** command. To revert to the default values, use the **no** form of this command.

**stopbits** { *1* | *2* }

**no stopbits** { *1* | *2* }

## Syntax Description

| | |
|---|---|
| **1** | Specifies one stop bit. |
| **2** | Specifies two stop bits. |

## Command Default

1 stop bit

## Command Modes

Line configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

## Usage Guidelines

You can configure the console ports only from a session on the console port.

## Examples

The following example shows how to configure the stop bits for the console port:

```
Device# configure terminal
Device(config)# line console 0
Device(config-line)# stopbits 1
```

# 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## 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.

**switchport access vlan** {*vlan-id* }
**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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## 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:

```
Device(config-if)# switchport access vlan 2
```

# 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## 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 nonegotiate** 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.

**tag rf** *rf-tag*

## Syntax Description

| | |
|---|---|
| *rf-tag* | RF tag name. |

## Command Default

None

## Command Modes

config-ap-filter

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to configure a policy tag for an AP filter:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap filter name ap-filter-name
Device(config-ap-filter)# rf tag rf-tag-name
```

# tag site

To configure a site tag for an AP filter, use the **tag site** *site-tag* command.

**tag site** *site-tag*

## Syntax Description

| | |
|---|---|
| *site-tag* | Name of the site tag. |

## Command Default

None

## Command Modes

config-ap-filter

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to configure a site tag for an AP filter:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap filter name ap-filter-name
Device(config-ap-filter)# site tag site-tag-name
```

# 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## 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:

```
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|PLUS|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.<br>The range is from 1 to 30 seconds.<br>**Note** The *public-key* and *resolver* parameter-map options are automatically populated with the default values. So, you need not change them. |

## Command Default

None

## Command Modes

Profile configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

### Example

This example shows how to configure timeout value for UDP sessions:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# parameter-map type umbrella global
Device(config-profile)# token 57CC80106C087FB1B2A7BAB4F2F4373C00247166
Device(config-profile)# local-domain dns_wl
Device(config-profile)# udp-timeout 2
Device(config-profile)# end
```

# umbrella-param-map

To configure the Umbrella OpenDNS feature for WLAN, use the **umbrella-param-map** command.

**umbrella-param-map** *umbrella-name*

### Syntax Description

| *umbrella-name* |
|---|

### Command Default

None

### Command Modes

config-wireless-policy

### Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

### Example

This example shows how to configure the Umbrella OpenDNS feature for WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy default-policy-profile
Device(config-wireless-policy)# umbrella-param-map global
Device(config-wireless-policy)# end
```

# update-timer

To configure the mDNS update timers for flex profile, use the **update-timer** command. To disable the command, use the **no** form of this command.

**update-timer** { **service-cache** *<1-100>* | **statistics** *<1-100>* }

**update-timer** { **service-cache** *<1-100>* | **statistics** *<1-100>* }

## Syntax Description

| | |
|---|---|
| **update-timer** | Configures the mDNS update timers for flex profile. |
| **service-cache** *<1-100>* | Specifies the mDNS update service-cache timer for flex profile. The default value is one minute, |
| **statistics** *<1-100>* | Specifies the mDNS update statistics timer for flex profile. The default value is one minute, |

## Command Default

None

## Command Modes

mDNS flex profile configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Amsterdam 17.3.1 | This command was introduced. |

## Examples

The following example shows how to configure the mDNS update timers for flex profile:

```
Device(config-mdns-flex-prof)# update-timer service-cache 20
```

# username

To add a user who can access the Cisco Catalyst 9800 Series Controller using SSH, use the **username** command in configuration mode. If the user already exists, the password, the privilege level, or both change with this command. To delete the user from the system, use the **no** form of this command.

**[no] username** *username* **password** {**hash** | **plain**} *password* **role** {**admin** | **user**] [**disabled** [**email** email-address]] [**email** email-address]

For an existing user, use the following command option:

**username** username **password role** {admin | **user**} password

## Syntax Description

| | |
|---|---|
| *username* | You should enter only one word which can include hyphen (-), underscore (_) and period (.).<br>**Note** Only alphanumeric characters are allowed at an initial setup. |
| **password** | The command to use specify password and user role. |
| *password* | Password character length up to 40 alphanumeric characters. You must specify the password for all new users. |
| **hash \| plain** | Type of password. Up to 34 alphanumeric characters. |
| **role admin \| user** | Sets the privilege level for the user. |
| **disabled** | Disables the user according to the user’s email address. |
| **email** *email-address* | The user’s email address. For example, user1@example.com. |
| **wlan-profile-name** | Displays details of the WLAN profile. |

## Command Default

The initial user during setup.

## Command Modes

Configuration

## Usage Guidelines

The **username** command requires that the username and password keywords precede the hash | plain and the admin | user options.

### Example 1

```
ncs/admin(config)# username admin password hash ###### role admin
ncs/admin(config)#
```

### Example 2

```
ncs/admin(config)# username admin password plain Secr3tp@swd role admin
ncs/admin(config)#
```

### Example 3

```
ncs/admin(config)# username admin password plain Secr3tp@swd role admin email
```

```
admin123@example.com
ncs/admin(config)#
```

# violation

To configure stream violation policy on periodic reevaluation, use the **violation** command.

**violation** {**drop** | **fallback**}

## Syntax Description

| Parameter | Description |
|---|---|
| **drop** | Stream will be dropped on periodic reevaluation. |
| **fallback** | Stream will be demoted to BestEffort class on periodic reevaluation. |

## Command Default

None

## Command Modes

config-media-stream

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to configure stream violation policy on periodic reevaluation:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless media-stream group my-media-group 224.0.0.0 224.0.0.223
Device(config-media-stream)# violation drop
```

# vlan

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.

**vlan** { *vlan-id* | **accounting** { **input** | **output** } | **configuration** *vlan-id* | **group** *word* **vlan-list** *vlan-id* | **internal allocation policy** { **ascending** | **descending** } }
**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. |
| **group** *word* **vlan-list** | Enables creation of the VLAN group. The VLAN group name may contain up to 32 characters and must commence with a letter. |
| **accounting** | VLAN accounting configuration. |
| **configuration** | VLAN feature configuration mode for advanced service parameters. One or more VLANs can be created for the same settings. *id* refers to the VLAN configuration ID. For example, 1-10 or 15. |
| **internal** | Internal VLAN allocation policy. It can be ascending or descending. |

## Command Default

None

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to configure a VLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# vlan 12
```

# 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

| 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 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## 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
```

# vlan filter

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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## 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 mac1 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** *vlan-list*
**no vlan group** *group-name* **vlan-list** *vlan-list*

## Syntax Description

| | |
|---|---|
| *group-name* | Name of the VLAN group. The group name may contain up to 32 characters and must begin with a letter. |
| **vlan-list** *vlan-list* | Specifies one or more VLANs to be added to the VLAN group. The *vlan-list* 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 (,). |

## Command Default

None

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to enable WGB broadcast tagging for a wireless policy profile:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy profile-policy-name
Device(config-wireless-policy)# wgb broadcast-tagging
```

# wgb vlan

To configure WGB VLAN client support for a WLAN policy profile, use the **wgb vlan** command.

**wgb vlan**

### Command Default

None

### Command Modes

config-wireless-policy

### Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to enable WGB VLAN client support for the WLAN policy profile named *wlan1-policy-profile*:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy wlan1-policy-profile
Device(config-wireless-policy)# wgb vlan
```

# whitelist acl

To configure the whitelist ACL, use the **whitelist acl** command.

**whitelist acl** {*standard_acl_value* | *extended_acl_value* | *acl_name*}

## Syntax Description

| | |
|---|---|
| *standard_acl_value* | Specifies the standard access list. Range is from 1 to 199. |
| *extended_acl_value* | Specifies the extended access list. Range is from 1300 to 2699. |
| *acl_name* | Specifies the named access list. |

## Command Default

None

## Command Modes

ET-Analytics configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to enable in-active timer in the ET-Analytics configuration mode:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# et-analytics
Device(config-et-analytics)# whitelist acl
eta-whitelist
Device((config-et-analytics)# ip access-list
extended eta-whitelist
Device(config-ext-nacl)# permit udp any any eq tftp
Device(config-ext-nacl)# end
```

# wired-vlan-range

To configure wired VLANs on which mDNS service discovery should take place, use the **wired-vlan-range** command. To disable the command, use the **no** form of this command.

**wired-vlan-range** *wired-vlan-range-value*

## Syntax Description

| | |
|---|---|
| **wired-vlan-range** | Configures wired VLANs on which mDNS service discovery should take place. |
| *wired-vlan-range-value* | Specifies the wired VLAN range value. |

## Command Default

None

## Command Modes

mDNS flex profile configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Amsterdam 17.3.1 | This command was introduced. |

## Examples

The following example shows how to configure wired VLANs on which mDNS service discovery should take place:

```
Device(config-mdns-flex-prof)# wired-vlan-range range-value
```

# config wlan assisted-roaming

To configure assisted roaming on a WLAN, use the **config wlan assisted-roaming** command.

**config wlan assisted-roaming** {**neighbor-list** | **dual-list** | **prediction**} {**enable** | **disable**} *wlan_id*

## Syntax Description

| | |
|---|---|
| **neighbor-list** | Configures an 802.11k neighbor list for a WLAN. |
| **dual-list** | Configures a dual band 802.11k neighbor list for a WLAN. The default is the band that the client is currently associated with. |
| **prediction** | Configures an assisted roaming optimization prediction for a WLAN. |
| **enable** | Enables the configuration on the WLAN. |
| **disable** | Disables the configuration on the WLAN. |
| *wlan_id* | Wireless LAN identifier between 1 and 512 (inclusive). |

## Command Default

The 802.11k neighbor list is enabled for all WLANs.

By default, dual band list is enabled if the neighbor list feature is enabled for the WLAN.

## Usage Guidelines

When you enable the assisted roaming prediction list, a warning appears and load balancing is disabled for the WLAN, if load balancing is already enabled on the WLAN.

The following example shows how to enable an 802.11k neighbor list for a WLAN:

```
(Cisco Controller) >config wlan assisted-roaming neighbor-list enable 1
```

# wireless aaa policy

To configure a wireless AAA policy, use the **wireless aaa policy** command.

**wireless aaa policy** *aaa-policy*

## Syntax Description

| | |
|---|---|
| *aaa-policy* | Name of the wireless AAA policy. |

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to configure a wireless AAA policy named *aaa-policy-test*

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless aaa policy aaa-policy-test
```

# wireless aaa policy

To configure a new AAA policy, use the **wireless aaa policy** command.

**wireless aaa policy** *aaa-policy-name*

## Syntax Description

| | |
|---|---|
| *aaa-policy-name* | AAA policy name. |

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to configure a AAA policy name:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless aaa policy my-aaa-policy
```

# wireless autoqos policy-profile

To enable the **autoqos** wireless policy with an executable command, use the autoqos command. Use the **disable** command to disable wireless AutoQos.

**wireless autoqos policy-profile***policy-profile-name* **default_policy_profile mode** { **clear** | **enterprise-avc** | **fastlane** | **guest** | **voice** }

**wireless autoqos disable**

### Syntax Description

| | |
|---|---|
| **autoqos** | Configures wireless Auto QoS. |
| **mode** | Specifies the wireless AutoQoS mode. |
| **enterprise-avc** | Enables AutoQos wireless enterprise AVC policy. |
| **clear** | Clears the configured wireless policy. |
| **fastlane** | Enables the AutoQos fastlane policy. This will disable and enable the 2.4GHz or 5GHz 802.11 network. |
| **guest** | Enables AutoQos wireless guest policy. |
| **voice** | Enables AutoQos wireless voice policy. This will disable and enable the 2.4GHz or 5GHz 802.11 network. |

### Command Default

None

### Command Modes

Privilege EXEC mode

### Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.12.2s | This command was introduced. |

### Example

This example shows how to enable AutoQoS wireless enterprise policy:

```
Device# wireless autoqos policy-profile default-policy-profile mode enterprise-avc
```

# wireless broadcast vlan

To enable broadcast support on a VLAN, use the **wireless broadcast vlan** command in global configuration mode. To disable Ethernet broadcast support, use the **no** form of the command.

**wireless broadcast vlan** [*vlan-id*]
**no wireless broadcast vlan** [*vlan-id*]

## Syntax Description

| | |
|---|---|
| *vlan-id* | (Optional) Specifies the VLAN ID to enable broadcast support to that VLAN. The value ranges from 1 to 4095. |

## Command Default

None

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

Use this command in the global configuration mode only.

This example shows how to enable broadcasting on VLAN 20:

```
Device(config)# wireless broadcast vlan 20
```

# wireless client

To configure client parameters, use the **wireless client** command in global configuration mode.

**wireless client** {**association limit** *assoc-number* **interval** *interval* | **band-select** {**client-mid-rssi** *rssi* | **client-rssi** *rssi* | **cycle-count** *count* | **cycle-threshold** *threshold* | **expire dual-band** *timeout* | **expire suppression** *timeout*} | **fast-ssid-change** | **max-user-login** *max-user-login* | **notification** {**interval** *time* | **join-failure aaathreshold***percentage* | **roam-failure threshold** *percentage*} | **timers auth-timeout** *seconds* | **user-timeout** *user-timeout*}

## Syntax Description

| | |
|---|---|
| **association limit** *assoc-number* **interval** *interval* | Enables association request limit per access point slot at a given interval and configures the association request limit interval.<br>You can configure number of association request per access point slot at a given interval from one through 100.<br>You can configure client association request limit interval from 100 through 10000 milliseconds. |
| **band-select** | Configures the band select options for the client. |
| **client-mid-rssi** *rssi* | Sets the client mid-rssi threshold for band select.<br>The minimum dBm of a client RSSI to respond to probe is between -90 and -20. |
| **client-rssi** *rssi* | Sets the client received signal strength indicator (RSSI) threshold for band select.<br>The minimum dBm of a client RSSI to respond to probe is between -90 and -20. |
| **cycle-count** *count* | Sets the band select probe cycle count.<br>You can configure the cycle count from 1 to 10. |
| **cycle-threshold** *threshold* | Sets the time threshold for a new scanning cycle.<br>You can configure the cycle threshold from 1 to 1000 milliseconds. |
| **expire dual-band** *timeout* | Sets the timeout before stopping to try to push a given client to the 5-GHz band.<br>You can configure the timeout from 10 to 300 seconds, and the default value is 60 seconds. |
| **expire suppression** *timeout* | Sets the expiration time for pruning previously known dual-band clients.<br>You can configure the suppression from 10 to 200 seconds, and the default timeout value is 20 seconds. |
| **fast-ssid-change** | Enables the fast SSID change for mobile stations. |
| **max-user-login** *max-user-login* | Configures the maximum number of login sessions for a user. |

| | |
|---|---|
| **notification** | Configures notifications. |
| **interval** *time* | Configures notifications for an interval.<br>The valid time ranges from 1 to 1440 seconds. |
| **join-failure aaa threshold** *percentage* | Configures notifications for client join failures.<br>You can configure the threshold percentage to trigger an alert. The valid threshold percentage ranges from 1 to 100. |
| **roam-failure threshold** *percentage* | Configures notifications for client roam failures.<br>You can configure the threshold for notifications. The valid threshold percentage ranges from 1 to 100. |
| **timers auth-timeout** *seconds* | Configures the client timers. |
| **user-timeout** *user-timeout* | Configures the idle client timeout. |

## Command Default

No default behavior or values.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |
| Cisco IOS XE Gibraltar 16.10.1 | This command was modified. The **client-mid-rssi, notification**, and **fast-ssid-change** keywords were added. The **user-timeout** keyword was deleted. |

This example shows how to set the proble cycle count for band select to 8:

```
Device# configure terminal
Device(config)# wireless client band-select cycle-count 8
Device(config)# end
```

This example shows how to set the time threshold for a new scanning cycle with threshold value of 700 milliseconds:

```
Device# configure terminal
Device(config)# wireless client band-select cycle-threshold 700
Device(config)# end
```

This example shows how to suppress dual-band clients from the dual-band database after 70 seconds:

```
Device# configure terminal
Device(config)# wireless client band-select expire suppression 70
Device(config)# end
```

# wireless client mac-address

To configure the wireless client settings, use the **wireless client mac-address** command in global configuration mode.

**wireless client mac-address** *mac-addr* **ccx** {**clear-reports** | **clear-results** | **default-gw-ping** | **dhcp-test** | **dns-ping** | **dns-resolve hostname** *host-name* | **get-client-capability** | **get-manufacturer-info** | **get-operating-parameters** | **get-profiles** | **log-request** {**roam** | **rsna** | **syslog**} | **send-message** *message-id* | **stats-request** *measurement-duration* {**dot11** | **security**} | **test-abort** | **test-association** *ssid bssid dot11 channel* | **test-dot1x** [*profile-id*] *bssid dot11 channel* | **test-profile** {**any***profile-id*}}

## Syntax Description

| | |
|---|---|
| *mac-addr* | MAC address of the client. |
| **ccx** | Cisco client extension (CCX). |
| **clear-reports** | Clears the client reporting information. |
| **clear-results** | Clears the test results on the controller. |
| **default-gw-ping** | Sends a request to the client to perform the default gateway ping test. |
| **dhcp-test** | Sends a request to the client to perform the DHCP test. |
| **dns-ping** | Sends a request to the client to perform the Domain Name System (DNS) server IP address ping test. |
| **dns-resolve hostname** *host-name* | Sends a request to the client to perform the Domain Name System (DNS) resolution test to the specified hostname. |
| **get-client-capability** | Sends a request to the client to send its capability information. |
| **get-manufacturer-info** | Sends a request to the client to send the manufacturer's information. |
| **get-operating-parameters** | Sends a request to the client to send its current operating parameters. |
| **get-profiles** | Sends a request to the client to send its profiles. |
| **log-request** | Configures a CCX log request for a specified client device. |
| **roam** | (Optional) Specifies the request to specify the client CCX roaming log |
| **rsna** | (Optional) Specifies the request to specify the client CCX RSNA log. |
| **syslog** | (Optional) Specifies the request to specify the client CCX system log. |

**send-message** *message-id*

Sends a message to the client.

Message type that involves one of the following:

- 1—The SSID is invalid
- 2—The network settings are invalid.
- 3—There is a WLAN credibility mismatch.
- 4—The user credentials are incorrect.
- 5—Please call support.
- 6—The problem is resolved.
- 7—The problem has not been resolved.
- 8—Please try again later.
- 9—Please correct the indicated problem.
- 10—Troubleshooting is refused by the network.
- 11—Retrieving client reports.
- 12—Retrieving client logs.
- 13—Retrieval complete.
- 14—Beginning association test.
- 15—Beginning DHCP test.
- 16—Beginning network connectivity test.
- 17—Beginning DNS ping test.
- 18—Beginning name resolution test.
- 19—Beginning 802.1X authentication test.
- 20—Redirecting client to a specific profile.
- 21—Test complete.
- 22—Test passed.
- 23—Test failed.
- 24—Cancel diagnostic channel operation or select a WLAN profile to resume normal operation.
- 25—Log retrieval refused by the client.
- 26—Client report retrieval refused by the client.
- 27—Test request refused by the client.
- 28—Invalid network (IP) setting.
- 29—There is a known outage or problem with the network.

- 30—Scheduled maintenance period.
- 31—The WLAN security method is not correct.
- 32—The WLAN encryption method is not correct.
- 33—The WLAN authentication method is not correct.

| | |
|---|---|
| **stats-request** *measurement-duration* | Senda a request for statistics. |
| **dot11** | Optional) Specifies dot11 counters. |
| **security** | (Optional) Specifies security counters. |
| **test-abort** | Sends a request to the client to abort the current test. |
| **test-association** *ssid bssid dot11 channel* | Sends a request to the client to perform the association test. |
| **test-dot1x** | Sends a request to the client to perform the 802.1x test. |
| *profile-id* | (Optional) Test profile name. |
| *bssid* | Basic SSID. |
| *dot11* | Specifies the 802.11a, 802.11b, or 802.11g network. |
| *channel* | Channel number. |
| **test-profile** | Sends a request to the client to perform the profile redirect test. |
| **any** | Sends a request to the client to perform the profile redirect test. |
| *profile-id* | Test profile name.<br>**Note** The profile ID should be from one of the client profiles for which client reporting is enabled. |

## Command Default

No default behavior or values.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

The **default-gw-ping** test does not require the client to use the diagnostic channel.

This example shows how to clear the reporting information of the client MAC address 00:1f:ca:cf:b6:60:

```
Device# configure terminal
```

```
Device(config)# wireless client mac-address 00:1f:ca:cf:b6:60 ccx clear-reports
Device(config)# end
```

# wireless client vlan-persistent

To enable client roaming across different policy profiles, use the **wireless client vlan-persistent** command.

**wireless client vlan-persistent**

**no wireless client vlan-persistent**

## Syntax Description

This command has no keywords or arguments.

## Command Default

None

## Command Modes

Global Configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Amsterdam 17.3.1 | This command was introduced. |

## Examples

The following example shows how to enable client roaming across different policy profiles:

```
Device(config) # wireless client vlan-persistent
```

# wireless config validate

To validate whether the wireless configuration is complete and consistent (all the functional profiles and tags are defined, and all the associations are complete and consistent), use the **wireless config validate** command in privileged EXEC mode.

**wireless config validate**

## Syntax Description

This command has no keywords or arguments.

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

In Cisco vEWLC, the wireless configuration is built using a collection of profiles, with each profile defining a functional block. These functional blocks are defined independently and is used to realize well-defined associations through intent based work-flows in building the wireless LAN. Such flexibility of modularizing the functional blocks requires the administrator to ensure that all associations are consistent and complete.

To ensure completeness and consistency of the wireless configuration, a configuration validation library is used to validate the configuration definitions across tables. The **wireless config validate** exec command is introduced from this release to validate the wireless configuration and report inconsistencies, if any, using contextual error message that is visible in btrace infra and on the console (if console logging is enabled). This command calls out any inconsistencies (unresolved associations) enabling you to realize a functional wireless LAN.

Use the following command to direct the output to a file: **show logging | redirect bootflash:** *filename* .

The following set of wireless configurations are validated:

| RF tag | Site tag | Policy tag | Policy profile | Flex profile |
|---|---|---|---|---|
| site-tag | flex-profile | wlan profile | IPv4 ACL name | VLAN ACL |
| poliy-tag | ap-profile | policy profile | Fabric name | ACL-policy |
| rf-tag | -— | -— | service-policy input and output name | RF Policy (5GHz and 24GHz) |
| -— | -— | -— | service-policy input and client output name | -— |

### Example

The following is sample output from the **wireless config validate** command

```
Device# wireless config validate

Oct 10 18:21:59.576 IST: %CONFIG_VALIDATOR_MESSAGE-5-EWLC_GEN_ERR: Chassis 1 R0/0: wncmgrd:
 Error in AP: fc99.473e.0a90  Applied site-tag : mysite definitiondoes not exist
Oct 10 18:21:59.576 IST: %CONFIG_VALIDATOR_MESSAGE-5-EWLC_GEN_ERR: Chassis 1 R0/0: wncmgrd:
 Error in AP: fc99.473e.0a90  Applied policy-tag : mypolicy definition does not exist
Oct 10 18:21:59.576 IST: %CONFIG_VALIDATOR_MESSAGE-5-EWLC_GEN_ERR: Chassis 1 R0/0: wncmgrd:
 Error in AP: fc99.473e.0a90  Applied rf-tag : myrf definition does not exist
```

# wireless country

To configure one or more country codes for a device, use the **wireless country** command.

**wireless** **country** *country-code*

## Syntax Description

| | |
|---|---|
| *country-code* | Two-letter country code. |

## Command Default

None

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Amsterdam 17.3.1 | This command was introduced. |

## Usage Guidelines

The Cisco must be installed by a network administrator or qualified IT professional and the installer must select the proper country code. Following installation, access to the unit should be password protected by the installer to maintain compliance with regulatory requirements and to ensure proper unit functionality. See the related product guide for the most recent country codes and regulatory domains.

This example shows how to configure country code on the device to IN (India):

```
Device(config)# wireless country IN
```

# wireless exclusionlist mac address

To manually add clients to the exclusionlist, use the wireless exclusion list command. To remove the manual entry, use the no form of the command.

**wireless exclusionlist** *mac_address* **description**

## Syntax Description

| | |
|---|---|
| **description** *value* | Configures the entry description. |

## Command Default

None

## Command Modes

Global Configuration

## Command History

| Cisco IOS XE Gibraltar 16.10.1 | Modification |
|---|---|
| | This command was introduced in this release. |

## Usage Guidelines

If a client was added to the exclusion list dynamically, the command to remove it is **wireless client mac-address xxxx.xxxx.xxxx deauthenticate** from enable mode.

### Example

This example shows how to manage exclusion entries:

```
Device(config)# wireless exclusion list xxxx.xxxx.xxxx
```

# wireless 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

## Usage Guidelines

If 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

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

| | |
|---|---|
| **control-plane** *control-plane-name* | Configure the control plane details. |
| **name** *vnid-map-name* | Configure the wireless fabric name |
| **l2-vnid** *id* | Configure the Layer 2 VNID. Valid range is 0 to 16777215. |
| **l3-vnid** *id* | Configure the Layer 3 VNID. Valid range is 0 to 16777215. |
| **ip** {*ipv4-addr netmask-addr* \| *ipv6-addr netmask-addr*} | IP address and netmask address details. |

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to configure 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 ipv6 ra wired

To enable the forwarding of Router Advertisement message to the wired clients, use the **wireless ipv6 ra wired** command.

**wireless ipv6 ra wired** { **nd** { **na-forward** | **ns-forward** } | **ra-wired** }

## Syntax Description

| | |
|---|---|
| *nd* | Configures wireless IPv6 ND parameters. |
| *na-forward* | Enables forwarding of Neighbor Advertisement to wireless clients. |
| *ns-forward* | Enable forwarding of Neighbor Solicitation to wireless clients. |
| *ra* | Configures wireless IPv6 Router Advertisement parameters. |
| *wired* | Enables forwarding of Router Advertisement message to the wired clients. |

## Command Default

None

## Command Modes

Global Configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.12.3 | This command was introduced. |

### Example

The following example shows how to enable the forwarding of Router Advertisement message to the wired clients:

```
Device(config)# wireless ipv6 ra wired
```

**Warning** The **wireless ipv6 ra wired** command must be enabled only for certification purpose and not during the deployment.

# wireless load-balancing

To globally configure aggressive load balancing on the controller, use the **wireless load-balancing** command in global configuration mode.

**wireless load-balancing** {**denial** *denial-count* | **window** *client-count*}

## Syntax Description

| | |
|---|---|
| **denial** *denial-count* | Specifies the number of association denials during load balancing.<br>Maximum number of association denials during load balancing is from 1 to 10 and the default value is 3. |
| **window** *client-count* | Specifies the aggressive load balancing client window, with the number of clients needed to trigger aggressive load balancing on a given access point.<br>Aggressive load balancing client window with the number of clients is from 0 to 20 and the default value is 5. |

## Command Default

Disabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

Load-balancing-enabled WLANs do not support time-sensitive applications like voice and video because of roaming delays.

When you use Cisco 7921 and 7920 Wireless IP Phones with controllers, make sure that aggressive load balancing is disabled on the voice WLANs for each controller. Otherwise, the initial roam attempt by the phone might fail, causing a disruption in the audio path.

This example shows how to configure association denials during load balancing:

```
Device# configure terminal
Device(config)# wireless load-balancing denial 5
Device(config)# end
```

# wireless macro-micro steering transition-threshold

To configure micro-macro transition thresholds, use the **wireless macro-micro steering transition-threshold** command.

**wireless macro-micro steering transition-threshold** {**balancing-window** | **client count** *number-clients* } {**macro-to-micro** | **micro-to-macro** *RSSI in dBm*}

## Syntax Description

| | |
|---|---|
| **balancing-window** | Active instance of the configuration in Route-processor slot 0. |
| **client** | Standby instance of the configuration in Route-processor slot 0. |
| *number-clients* | Valid range is 0 to 65535 clients. |
| **macro-to-micro** | Configures the macro to micro transition RSSI. |
| **micro-to-macro** | Configures micro-macro client load balancing window. |
| *RSSI in dBm* | RSSI in dBm. Valid range is –128 to 0. |

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to configure balancing-window:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless macro-micro steering transition-threshold balancing-window
number-of-clients
```

# wireless macro-micro steering probe-suppression

To configure micro-macro probe suppressions, use the **wireless macro-micro steering probe-suppression** command.

**wireless macro-micro steering probe-suppression** {**aggressiveness** *number-of-cycles* | | **hysteresis***RSSI in dBm* | **probe-auth** | **probe-only**}

## Syntax Description

| | |
|---|---|
| **aggressiveness** | Configures probe cycles to be suppressed. The number of cycles range between 0 - 255. |
| **hysteresis** | Indicate show much greater the signal strength of a neighboring access point must be in order for the client to roam to it. The RSSI decibel value ranges from -6 to -3. |
| **probe-auth** | Enables mode to suppress probes and single auth |
| **probe-only** | Enables mode to suppress only probes |

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

### Examples

The following example shows how to configure balancing-window:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless macro-micro steering probe-suppression aggressiveness
number-of-cycles
```

# wireless management certificate

To create a wireless management certificate details, use the **wireless management certificate** command.

**wireless management certificate ssc** {**auth-token** {**0** | **8**} *token* | **trust-hash** *hash-key* }

## Syntax Description

| | |
|---|---|
| **auth-token** | Authentication token. |
| *token* | Token name. |
| **trust-hash** | Trusted SSC hash list. |
| *hash-key* | SHA1 fingerprint. |
| **0** | Specifies an UNENCRYPTED token. |
| **8** | Specifies an AES encrypted token. |

## Command Default

None

## Command Modes

Global Configuration(config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Example

The following example shows how to configure a wireless management certificate:

```
Device# configure terminal
Device(config)# wireless management certificate ssc trust-hash test
```

# wireless management interface

To create a wireless management interface, use the **wireless management interface** command.

**wireless management interface** {**GigabitEthernet** | **Loopback** | **Vlan** }*interface-number*

## Syntax Description

| | |
|---|---|
| *interface-number* | Interface number. |

## Command Default

None

## Command Modes

Global Configuration(config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Example

The following example shows how to configure a wireless management interface:

```
Device# configure terminal
Device(config)# wireless management interface vlan vlan1
```

# wireless management trustpoint

To create a wireless management trustpoint, use the **wireless management trustpoint** command.

**wireless management trustpoint** *trustpoint-name*

## Syntax Description

| | |
|---|---|
| *trustpoint-name* | Trustpoint name. |

## Command Default

None

## Command Modes

Global Configuration(config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

## Usage Guidelines

Use this command only on the Cisco Catalyst 9800 Wireless Controller for Cloud platform and not on appliances as the appliances use the SUDI certificate by default without the need for this command.

### Example

The following example shows how to configure a wireless management trustpoint:

```
Device# configure terminal
Device(config)# wireless management trustpoint test
```

# wireless media-stream

To configure various parameters, use the **wireless media-stream** command.

**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

| | |
|---|---|
| **group** *groupName* | Configure multicast-direct status for a group. |
| *startipAddr* | Specifies the start IP Address for the group. |
| *endipAddr* | Specifies the End IP Address for the group. |
| **group** *avg-packet-size* | Configure average packet size.<br>The values can range between 100 to 1500. |
| **group** *default* | Set a command to its defaults. |
| **group** *exit* | Exit sub-mode. |
| **group** *max-bandwidth* | Configure maximum expected stream bandwidth in Kbps.<br>The values can range between 1 to 35000 kbps. |
| **group** *no* | Negate a command or set its defaults. |
| **group** *policy* | Configure media stream admission policy.<br>You can choose either of these options:<br>• admit - Allow traffic for the media stream group.<br>• deny - Deny traffic for the media stream group. |
| **group** *qos* | Configure over the air QoS class, <'video'> ONLY. |
| **multicast-direct** | Configure multicast-direct status. |
| **message** | Configure Session Announcement Message. |
| **phone** *phone* | Configure Session Announcement Phone number. |
| **URL** *URL* | Configure Session Announcement URL. |
| **Notes** *Notes* | Configure Session Announcement notes. |
| **Email** *Email* | Configure Session Announcement Email. |

## Command Default

Disabled

## Command Modes

config

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was modified. |

## 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

| | |
|---|---|
| **Email** | Configure session announcement e-mail. |
| **Notes** | Configure session announcement notes. |
| **URL** | Configure session announcement URL. |
| **phone** | Configure session announcement phone number. |

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

## 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**

## Command Default

None

## Command Modes

config

## Usage Guidelines

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.

### 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** command.

**wireless mesh alarm association count** *count*

## Syntax Description

| | |
|---|---|
| *count* | Number of alarm associations. The vlaid range is between 1 and 30. |

## Command Default

None

## Command Modes

config

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to configure the 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.

**wireless 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to configure the mesh 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to configure the mesh 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to configure the mesh 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to configure the mesh 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 paramter, 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to configure the mesh 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to configure the 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.

**wireless mesh backhaul bdomain-channels**

## Syntax Description

| | |
|---|---|
| **bdomain-channels** | Allows the Extended UNII B Domain channels for Outdoor mesh APs backhaul radio.<br>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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to disable the 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

| 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 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to configure the mesh 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

| | |
|---|---|
| **ethernet-bridging** | Configure ethernet bridging. |
| **allow-bdpu** | Configures STP BPDUs towards wired MESH uplink. |

## Command Default

None

## Command Modes

config

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to configure 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.

**wireless mesh security psk provisioning** {**default_psk** | **inuse** *psk-index* | **key** *psk-index* {**0** | **8**}*enter-psk-name psk-description*}

## Syntax Description

| | |
|---|---|
| **provisioning** | configuring mesh psk provisioning parameters. |
| **default_psk** | Set the mesh provisioning to the default-psk settings. |
| **inuse** | Configuring the psk inuse index |
| *psk-index* | Enter PSK key index. Valid range is between 1 and 5. |
| **key** | Configure a pre-shared-key |
| *psk-index* | Enter PSK key index. Valid range is between 1 and 5. |
| **0** | Choose to enter an UNENCRYPTED password. |
| **8** | Choose to enter an AES encrypted password. |
| *enter-psk-name* | Enter a name for the configured psk key. |
| *psk-description* | Enter a description for this key. |

## Command Default

None

## Command Modes

config

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to provision the default psk key for the mesh security:

```
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.

**wireless mesh subset-channel-sync**

### Syntax Description

| | |
|---|---|
| **subset-channel-sync** | Configures the subset channel sync for mobility group |

### Command Default

None

### Command Modes

config

### Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to configure 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shoes 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**

## Syntax Description

| | |
|---|---|
| *peer group* | Name of the peer group. |
| **member IP** | Adds a peer group member. |
| *ip-address* | IP address of the peer group member to be added. |
| **mode centralized** | Configures the management mode of the peer group member as centrally managed. |

## Command Default

The centralized mode is off.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE 3.7.0 E | This command was introduced. |

```
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** *numbe r* | **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.<br>**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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to configure a 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

| | |
|---|---|
| *ip-address* | The IP address of the member controller. |
| **public-ip** *public-ip-address* | (Optional) Member controller public IP address.<br>**Note** This command is used only when the member is behind a NAT. Only static IP NAT is supported. |
| **group** *group-name* | (Optional) Member controller group name.<br>**Note** 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to configure a 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 hte 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.

**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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to configure a mobility domain name lab1:

```
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

| 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 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to configure a 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.

**wireless multicast** {*ipv4-address* | **ipv6** *ipv6-address* | **non-ip** [**vlan** *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.<br>Valid range for VLAN ID is 1 to 4094. |

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to configure a 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

### Example

The following example shows how to configure the AP packet capture profile:

```
Device(config)# wireless profile ap packet-capture test1
```

# wireless profile fabric

To configure the fabric profile parameters, use the **wireless profile fabric** command.

**wireless profile fabric** *fabric-profile-name*

## Syntax Description

| | |
|---|---|
| *fabric-profile-name* | Fabric profile name. |
| **fabric** | Configure Fabric profile parameters. |
| **profile** | Configure profile parameters. |

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to configure the 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to configure a WLAN policy profile:

```
Device(config)# wireless profile policy mywlan-profile-policy
```

# wireless rfid

To set the static radio-frequency identification (RFID) tag data timeout value, use the **wireless rfid** command in global configuration mode.

**wireless rfid timeout** *timeout-value*

## Syntax Description

| | |
|---|---|
| **timeout** | Configures the static RFID tag data timeout value. |
| *timeout-value* | RFID tag data timeout value. Valid values range from 60-7200. |

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

### Example

This example shows how to set the static RFID tag data timeout value.

```
Device(config)# wireless rfid timeout 70
```

# wireless security dot1x

To configure IEEE 802.1x global configurations, use the **wireless security dot1x** command.

**wireless security dot1x** [**eapol-key** {**retries** *retries* | **timeout** *milliseconds*} | **group-key interval** *sec* | **identity-request** {**retries** *retries* | **timeout** *seconds*} | **radius** [**call-station-id**] {**ap-macaddress** | **ap-macaddress-ssid** | **ipaddress** | **macaddress**} | **request** {**retries** *retries* | **timeout** *seconds*} | **wep key** {**index 0** | **index 3**}]

## Syntax Description

| | |
|---|---|
| **eapol-key** | Configures eapol-key related parameters. |
| **retries** *retries* | (Optional) Specifies the maximum number of times (0 to 4 retries) that the controller retransmits an EAPOL (WPA) key message to a wireless client.<br>The default value is 2. |
| **timeout** *milliseconds* | (Optional) Specifies the amount of time (200 to 5000 milliseconds) that the controller waits before retransmitting an EAPOL (WPA) key message to a wireless client using EAP or WPA/WPA-2 PSK.<br>The default value is 1000 milliseconds. |
| **group-key interval** *sec* | Configures EAP-broadcast key renew interval time in seconds (120 to 86400 seconds). |
| **identity-request** | Configures EAP ID request related parameters. |
| **retries** *retries* | (Optional) Specifies the maximum number of times (0 to 4 retries) that the controller request the EAP ID.<br>The default value is 2. |
| **timeout** *seconds* | (Optional) Specifies the amount of time (1 to 120 seconds) that the controller waits before retransmitting an EAP Identity Request message to a wireless client.<br>The default value is 30 seconds. |
| **radius** | Configures radius messages. |
| **call-station-id** | (Optional) Configures Call-Station Id sent in radius messages. |
| **ap-macaddress** | Sets Call Station Id Type to the AP's MAC Address. |
| **ap-macaddress-ssid** | Sets Call Station Id Type to 'AP MAC address':'SSID'. |
| **ipaddress** | Sets Call Station Id Type to the system's IP Address. |
| **macaddress** | Sets Call Station Id Type to the system's MAC Address. |
| **request** | Configures EAP request related parameters. |

| | |
|---|---|
| **retries** *retries* | (Optional) For EAP messages other than Identity Requests or EAPOL (WPA) key messages, specifies the maximum number of times (0 to 20 retries) that the controller retransmits the message to a wireless client.<br>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.<br>The default value is 30 seconds. |
| **wep key** | Configures 802.1x WEP related paramters. |
| **index 0** | Specifies the WEP key index value as 0 |
| **index 3** | Specifies the WEP key index value as 3 |

## Command Default

Default for eapol-key-timeout: 1 second.

Default for eapol-key-retries: 2 retries.

## Command Modes

config

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

None.

This example lists all the commands under **wireless security dot1x** .

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#wireless security dot1x ?
  eapol-key         Configure eapol-key related parameters
  group-key         Configures EAP-broadcast key renew interval time in seconds
  identity-request  Configure EAP ID request related parameters
  radius            Configure radius messages
  request           Configure EAP request related parameters
  wep               Configure 802.1x WEP related paramters
  <cr>
```

# wireless security dot1x radius accounting mac-delimiter

To configure a MAC delimiter for called-station-ID or a calling-station-ID, use the **wireless security dot1x radius accounting mac-delimiter** command.

To remove MAC delimiter for a called-station-ID or a calling-station-ID, use the **no** form of the command.

**wireless security dot1x radius accounting mac-delimiter** {**colon** | **hyphen** | **none** | **single-hyphen** }

## Syntax Description

| | |
|---|---|
| **colon** | Sets the delimiter to colon. |
| **hyphen** | Sets the delimiter to hyphen. |
| **none** | Disables delimiters. |
| **single-hyphen** | Sets the delimiters to single hyphen. |

## Command Default

None

## Command Modes

Global Configuration Mode

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE 3.6.0 E | This command was introduced. |

This example shows how to configure a MAC delimiter for called-station-ID or a calling-station-ID to colon:

```
Device(config)# wireless security dot1x radius accounting mac-delimiter colon
```

# wireless security dot1x radius accounting username-delimiter

To set the delimiter type, use **wireless security dot1x radius accounting username-delimiter** command, to remove the configuration, use the **no** form of this command.

**wireless security dot1x radius accounting username-delimiter** {**colon** | **hyphen** | **none** | **single-hyphen**}

## Syntax Description

| | |
|---|---|
| **colon** | Sets the delimiter to colon. |
| **hyphen** | Sets the delimiter to hyphen. |
| **none** | Disables delimiters. |
| **single-hyphen** | Sets the delimiters to single hyphen. |

## Command Default

None

## Command Modes

Global Configuration Mode.

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE 3.7.2 E | This command was introduced. |

This example shows how to sets the delimiter to colon.

```
Device(config)# wireless security dot1x radius acounting username-delimiter colon
```

# wireless security dot1x radius callStationIdCase

To configure Call Station Id CASE send in RADIUS messages, use the **wireless security dot1x radius callStationIdCase** command.

To remove the Call Station Id CASE send in RADIUS messages, use the **no** form of the command.

**wireless security dot1x radius callStationIdCase** {**lower** | **upper**}

## Syntax Description

| | |
|---|---|
| **lower** | Sends all Call Station Ids to RADIUS in lowercase |
| **upper** | Sends all Call Station Ids to RADIUS in uppercase |

## Command Default

None

## Command Modes

Global Configuration Mode

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE 3.6.0 E | This command was introduced. |

This example shows how to configure Call Station Id CASE send in RADIUS messages in lowercase:

```
Device(config)# wireless security dot1x radius callstationIdCase lower
```

# wireless security dot1x radius mac-authentication call-station-id

To configure call station ID type for mac-authentication, use the **wireless security dot1x radius mac-authentication call-station-id** command. To remove the configuration, use the **no** form of it.

**wireless security dot1x radius mac-authentication call-station-id ap-ethmac-only | ap-ethmac-ssid | ap-group-name | ap-label-address | ap-label-address-ssid | ap-location | ap-macaddress | ap-macaddress-ssid | ap-name | ap-name-ssid | ipaddress | macaddress | vlan-id**

## Syntax Description

| | |
|---|---|
| **ap-ethmac-only** | Sets call station ID type to the AP Ethernet MAC address. |
| **ap-ethmac-ssid** | Sets call station ID type to the format 'AP Ethernet MAC address':'SSID'. |
| **ap-group-name** | Sets call station ID type to the AP Group Name. |
| **ap-label-address** | Sets call station ID type to the AP MAC address on AP Label. |
| **ap-label-address-ssid** | Sets call station ID type to the format 'AP Label MAC address': 'SSID'. |
| **ap-location** | Sets call station ID type to the AP Location. |
| **ap-macaddress** | Sets call station ID type to the AP Radio MAC Address. |
| **ap-macaddress-ssid** | Sets call station ID type to the 'AP radio MAC Address':'SSID'. |
| **ap-name** | Sets call station ID type to the AP name. |
| **ap-name-ssid** | Sets call station ID type to the format 'AP name':'SSID'. |
| **ipaddress** | Sets call station ID type to the system IP Address. |
| **macaddress** | Sets call station ID type to the system MAC Address. |
| **vlan-id** | Sets call station ID type to the VLAN ID. |

## Command Default

None

## Command Modes

Global Configuration Mode

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE 3.7.2 E | This command was introduced. |

The example show how to set call station ID type to the AP Ethernet MAC address:

```
Device(config)# wireless security dot1x radius mac-authentication call-station-id
ap-ethmac-only
```

# wireless security dot1x radius mac-authentication mac-delimiter

To configure MAC-Authentication attributes, use the **wireless security dot1x radius mac-authentication mac-delimiter** command.

To remove MAC-Authentication attributes, use the **no** form of the command.

**wireless security dot1x radius mac-authentication mac-delimiter** {**colon** | **hyphen** | **none** | **single-hyphen** }

## Syntax Description

| | |
|---|---|
| **colon** | Sets the delimiter to colon. |
| **hyphen** | Sets the delimiter to hyphen. |
| **none** | Disables delimiters. |
| **single-hyphen** | Sets the delimiters to single hyphen. |

## Command Default

None

## Command Modes

Global Configuration Mode

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE 3.6.0 E | This command was introduced. |

This example shows how to configure MAC-Authentication attributes to colon:

```
Device(config)# Scurity dot1x radius mac-authentication mac-delimiter colon
```

# wireless security web-auth retries

To enable web authentication retry on a particular WLAN, use the **wireless wireless security web-auth retries** command. To disable, use the **no** form of the command.

**wireless securityweb-authretries***retries*
**nowireless securityweb-authretries**

## Syntax Description

| | |
|---|---|
| **wireless security web-auth** | Enables web authentication on a particular WLAN. |
| **retries** *retries* | Specifies maximum number of web authentication request retries. The range is from 0 through 30. The default value is 3. |

## Command Default

## Command Modes

config

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

None.

This example shows how to enable web authentication retry on a particular WLAN.

```
Device#configure terminal
Device# wireless security web-auth retries 10
```

# wireless tag policy

To configure wireless tag policy, use the **wireless tag policy** command.

**wireless tag policy** *policy-tag*

## Syntax Description

| | |
|---|---|
| *policy-tag* | Name of the wireless tag policy. |

## Command Default

The default policy tag is default-policy-tag.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to configure a wireless policy tag:

```
Device(config)# wireless tag policy guest-policy
```

# wireless tag site

To configure a wireless site tag, use the **wireless tag site** *site-tag*command.

**wireless tag site** *site-tag*

## Syntax Description

| | |
|---|---|
| *site-tag* | Name of the site tag. |

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

### Example

The following example shows how to configure a site tag:

```
Device(config)# wireless tag site test-site
```

# wireless wps ap-authentication

To configure the access point neighbor authentication, use the **wireless wps ap-authentication** command. To remove the access point neighbor authentication, use the no form of the command.

**wireless wps ap-authentication** [**threshold** *value*]
**no wireless wps ap-authentication** [**threshold**]

## Syntax Description

| | |
|---|---|
| **threshold** *value* | Specifies that the WMM-enabled clients are on the wireless LAN. Threshold value (1 to 255). |

## Command Default

None.

## Command Modes

config

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

None.

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 ap-authentication threshold

To configure the alarm trigger threshold for access point neighbor authentication, use the **wireless wps ap-authentication threshold** command. To remove the access point neighbor authentication, use the no form of the command.

**wireless wps ap-authentication threshold** *value*

**no wireless wps ap-authentication threshold** *value*

## Syntax Description

| | |
|---|---|
| **threshold** *value* | Specifies that the WMM-enabled clients are on the wireless LAN. The threshold value range is between 1 and 255. The default value is 1. |

## Command Default

None

## Command Modes

Global Configuration mode

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Amsterdam 16.12.1 | This command was introduced. |

## Usage Guidelines

None

### Example

The following example shows you how to configure the alarm trigger threshold for access point neighbor authentication:

```
Device(config)# wireless wps ap-authentication threshold 1
```

# wireless wps client-exclusion

To configure client exclusion policies, use the **wireless wps client-exclusion** command. To remove the client exclusion policies, use the **no** form of the command.

**wireless wps client-exclusion** {**all** | **dot11-assoc** | **dot11-auth** | **dot1x-auth** | **dot1x-timeout** | **ip-theft** | **web-auth**}
**no wireless wps client-exclusion** {**all** | **dot11-assoc** | **dot11-auth** | **dot1x-auth** | **dot1x-timeout** | **ip-theft** | **web-auth**}

## Syntax Description

| | |
|---|---|
| **dot11-assoc** | Specifies that the controller excludes clients on the sixth 802.11 association attempt, after five consecutive failures. |
| **dot11-auth** | Specifies that the controller excludes clients on the sixth 802.11 authentication attempt, after five consecutive failures. |
| **dot1x-auth** | Specifies that the controller excludes clients on the sixth 802.11X authentication attempt, after five consecutive failures. |
| **dot1x-timeout** | Enables exclusion on timeout and no response. |
| **ip-theft** | Specifies that the control excludes clients if the IP address is already assigned to another device.<br>For more information, see the Usage Guidelines section. |
| **web-auth** | Specifies that the controller excludes clients on the fourth web authentication attempt, after three consecutive failures. |
| **all** | Specifies that the controller excludes clients for all of the above reasons. |

## Command Default

Enabled.

## Command Modes

config

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

In IP-theft scenarios, there are differences between the older Cisco IOS XE releases and the Cisco IOS XE Denali 16.x releases:

| Older Cisco IOS XE Releases | Cisco IOS XE Denali 16.x Releases |
|---|---|
| Priority wise, wired clients have higher priority over wireless clients, and DHCP IP has higher priority over static IP. The client security type is not checked; security of all client types are treated with same priority.<br>If the existing binding is from a higher priority source, the new binding is ignored and an IP-theft is signaled. If the existing binding has the same source-priority as the new binding, the binding is ignored and an IP-theft is signaled. This ensures that the bindings are not toggled if two hosts send traffic using the same IP. Only the initial binding is retained in the software. If the new binding is from a higher priority source, the existing binding is replaced. This results in an IP-theft notification of existing binding and also a new binding notification. | There is not really a fundamental difference between wired and wireless; what matters is the trust (preflevel) of the entry, which is a function on how it was learnt (ARP, DHCP, ND, and so on) and the policy that is attached to the port. When preflevel is equal, the IP takeover is denied if the old entry is still reachable. IP takeover occurs when the update comes from a trusted port or a new entry gets IP from the DHCP server. Otherwise, you must explicitly grant it. The IP-theft is not reported if an old entry is replaced by a new and a more trusted one. |

This example shows how to disable clients on the 802.11 association attempt after five consecutive failures.

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#wireless wps client-exclusion dot11-assoc
```

# wireless wps mfp ap-impersonation

To configure AP impersonation detection, use the **wireless wps mfp ap-impersonation** command. Use the **no** form of this command to disable the configuration.

**wireless wps mfp ap-impersonation**

**no wireless wps mfp ap-impersonation**

## Syntax Description

| | |
|---|---|
| **ap-impersonation** | Configures AP impersonation detection. |

## Command Default

None

## Command Modes

Global Configuration mode

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Amsterdam 16.12.1 | This command was introduced. |

## Usage Guidelines

None

### Example

The following example shows you how to configure AP impersonation detection:

```
Device(config)# wireless wps mfp ap-impersonation
```

# wireless wps rogue

To configure various rouge parameters, use the **wireless wps rogue** command.

**wireless wps rogue** {**adhoc** | **client**} [**alert** *mac-addr* | **contain** *mac-addr* *no-of-aps*]

## Syntax Description

| | |
|---|---|
| **adhoc** | Configures the status of an Independent Basic Service Set (IBSS or ad-hoc) rogue access point. |
| **client** | Configures rogue clients |
| **alert** *mac-addr* | 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. |
| **contain** *mac-addr* *no-of-aps* | Contains the offending device so that its signals no longer interfere with authorized clients.<br>Maximum number of Cisco access points assigned to actively contain the ad-hoc rogue access point (1 through 4, inclusive). |

## Command Default

None.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

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 CNTL/Z.
Device(config)#wireless wps rouge adhoc alert mac_addr
```

# wireless wps rogue network-assurance enable

To enable the rogue wireless service assurance (WSA) events, use the **wireless wps rogue network-assurance enable** command. Use the **no** form of this command to disable the configuration.

**wireless wps rogue network-assurance enable**

**no wireless wps rogue network-assurance enable**

## Syntax Description

| | |
|---|---|
| **network-assurance enable** | Enables rogue WSA events. |

## Command Default

None

## Command Modes

Global Configuration mode

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Amsterdam 16.12.1 | This command was introduced. |

## Usage Guidelines

None

### Example

The following example shows you how to enable the rogue wireless service assurance events:

```
Device(config)# wireless wps rogue network-assurance enable
```

# wireless wps rogue ap aaa

To configure the use of AAA/local database to detect valid AP MAC addresses, use the **wireless wps rogue ap aaa** command. Use the **no** form of this command to disable the configuration.

**wireless wps rogue ap aaa**

**no wireless wps rogue ap aaa**

## Syntax Description

| | |
|---|---|
| **aaa** | Configures the use of AAA or local database to detect valid AP MAC addresses. |

## Command Default

None

## Command Modes

Global Configuration mode

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Amsterdam 16.12.1 | This command was introduced. |

## Usage Guidelines

None

### Example

The following example shows you how to configure the use of AAA/local database to detect valid AP MAC addresses:

```
Device(config)# wireless wps rogue ap aaa
```

# wireless wps rogue ap aaa polling-interval

To configures Rogue AP AAA validation interval, in seconds, use the **wireless wps rogue ap aaa polling-interval** command. To disable the configuration, use the no form of this command.

**wireless wps rogue ap aaa polling-interval** *60 - 86400*

**no wireless wps rogue ap aaa polling-interval** *60 - 86400*

## Syntax Description

| | |
|---|---|
| **aaa** | Sets the use of AAA or local database to detect valid AP MAC addresses. |
| **polling-interval** | Configures the rogue AP AAA validation interval. |
| *60 - 86400* | Specifies AP AAA validation interval, in seconds. |

## Command Default

None

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.12.1 | This command was introduced. |

## Usage Guidelines

None

### Example

This example shows how to configures Rogue AP AAA validation interval, in seconds:

```
Device(config)# wireless wps rogue ap aaa polling-interval 120
```

# wireless wps rogue ap init-timer

To configure the init timer for rogue APs, use the **wireless wps rogue ap init-timer** command. Use the **no** form of this command to disable the configuration.

**wireless wps rogue ap init-timer**

**no wireless wps rogue ap init-timer**

## Syntax Description

| | |
|---|---|
| **init-timer** | Configures the init timer for rogue APs. |

## Command Default

None

## Command Modes

Global Configuration mode

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Amsterdam 16.12.1 | This command was introduced. |

## Usage Guidelines

None

### Example

The following example shows you how to configure the init timer for rogue APs:

```
Device(config)# wireless wps rogue ap init-timer
```

# wireless wps rogue ap mac-address rldp initiate

To initiate and configure Rogue Location Discovery Protocol on rogue APs, use the **wireless wps rogue ap mac-address rldp initiate** command.

**wireless wps rogue ap mac-address** *<MAC Address>* **rldp initiate**

## Syntax Description

| | |
|---|---|
| **wps** | Configures the WPS settings. |
| **rogue** | Configures the global rogue devices. |
| **ap mac-address** *<MAC Address>* | The MAC address of the APs. |
| **rldp initiate** | Initiates RLDP on rogue APs. |

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Amsterdam 16.12.1 | This command was introduced. |

## Usage Guidelines

None

### Example

The following example shows you how to initiate and configure Rogue Location Discovery Protocol on rogue APs:

```
Device# wireless wps rogue ap mac-address 10.1.1 rldp initiate
```

# wireless wps rogue ap notify-min-rssi

To configure the minimum RSSI notification threshold for rogue APs, use the **wireless wps rogue ap notify-min-rssi** command. Use the **no** form of this command to disable the configuration.

**wireless wps rogue ap notify-min-rssi**

**no wireless wps rogue ap notify-min-rssi**

## Syntax Description

| | |
|---|---|
| **notify-min-rssi** | Configure the minimum RSSI notification threshold for rogue APs. |

## Command Default

None

## Command Modes

Global Configuration mode

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Amsterdam 16.12.1 | This command was introduced. |

## Usage Guidelines

None

### Example

The following example shows you how to configure the minimum RSSI notification threshold for rogue APs:

```
Device(config)# wireless wps rogue ap notify-min-rssi
```

# wireless wps rogue ap notify-rssi-deviation

To configure the RSSI deviation notification threshold for rogue APs, use the **wireless wps rogue ap notify-rssi-deviation** command. Use the **no** form of this command to disable the configuration.

**wireless wps rogue ap notify-rssi-deviation**

**no wireless wps rogue ap notify-rssi-deviation**

## Syntax Description

| | |
|---|---|
| **notify-rssi-deviation** | Configures the RSSI deviation notification threshold for rogue APs. |

## Command Default

None

## Command Modes

Global Configuration mode

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Amsterdam 16.12.1 | This command was introduced. |

## Usage Guidelines

None

### Example

The following example shows you how to configure the RSSI deviation notification threshold for rogue APs:

```
Device(config)# wireless wps rogue ap notify-rssi-deviation
```

# wireless wps rogue ap rldp alarm-only

To set Rogue Location Discovery Protocol (RLDP) and alarm if rogue is detected, use the **wireless wps rogue ap rldp alarm-only** command. Use the **no** form of this command to disable the configuration.

**wireless wps rogue ap rldp alarm-only**

**no wireless wps rogue ap rldp alarm-only**

## Syntax Description

| | |
|---|---|
| **alarm-only** | Sets RLDP and alarm if rogue is detected. |

## Command Default

None

## Command Modes

Global Configuration mode

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Amsterdam 16.12.1 | This command was introduced. |

## Usage Guidelines

None

### Example

The following example shows you how to set RLDP and alarm if rogue is detected:

```
Device(config)# wireless wps rogue ap rldp alarm-only
```

# wireless wps rogue ap rldp alarm-only monitor-ap-only

To perform RLDP only on monitor APs, use the **wireless wps rogue ap rldp alarm-only monitor-ap-only** command. Use the **no** form of this command to disable the configuration.

**wireless wps rogue ap rldp alarm-only monitor-ap-only**

**no wireless wps rogue ap rldp alarm-only monitor-ap-only**

## Syntax Description

| | |
|---|---|
| **monitor-ap-only** | Performs RLDP on monitor APs only. |

## Command Default

None

## Command Modes

Global Configuration mode

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Amsterdam 16.12.1 | This command was introduced. |

## Usage Guidelines

None

### Example

The following example shows you how to perform RLDP only on monitor APs,:

```
Device(config)# wireless wps rogue ap rldp alarm-only monitor-ap-only
```

# wireless wps rogue ap rldp auto-contain

To configure RLDP, alarm and auto-contain if rogue is detected, use **wirelesswps rogueaprldp auto-contain** command. Use the **no** form of the command to disable the alarm.

**[no] wireless wps rogue ap rldp auto-contain monitor-ap-only**

## Syntax Description

| | |
|---|---|
| **monitor-ap-only** | Perform RLDP only on monitor AP |

## Command Default

None

## Command Modes

Global Configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |
| Cisco IOS XE 3.7.3E | The **no** form of the command was introduced. |

### Example

This example shows how to configure an alarm for a detected rogue.

```
Devicewireless wps rogue ap rldp auto-contain
```

# wireless wps rogue ap rldp retries

To configure RLDP retry times on rogue APs, use the **wireless wps rogue ap rldp retries** command. Use the **no** form of this command to disable the configuration.

**wireless wps rogue ap rldp retries**

**no wireless wps rogue ap rldp retries**

## Syntax Description

| | |
|---|---|
| **retries** | Configures RLDP retry times on rogue APs. |

## Command Default

None

## Command Modes

Global Configuration mode

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Amsterdam 16.12.1 | This command was introduced. |

## Usage Guidelines

None

### Example

The following example shows you how to configure RLDP retry times on rogue APs:

```
Device(config)# wireless wps rogue ap rldp retries
```

# wireless wps rogue ap rldp schedule

To configure RLDP scheduling, use the **wireless wps rogue ap rldp schedule** command. Use the **no** form of this command to disable the configuration.

**wireless wps rogue ap rldp schedule**

**no wireless wps rogue ap rldp schedule**

## Syntax Description

| | |
|---|---|
| **schedule** | Configures RLDP scheduling. |

## Command Default

None

## Command Modes

Global Configuration mode

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Amsterdam 16.12.1 | This command was introduced. |

## Usage Guidelines

None

### Example

The following example shows you how to configure RLDP scheduling:

```
Device(config)# wireless wps rogue ap rldp schedule
```

# wireless wps rogue ap rldp schedule day

To configure the day when RLDP scheduling is to be done, use the **wireless wps rogue ap rldp schedule day** command. Use the **no** form of this command to disable the configuration.

**wireless wps rogue ap rldp schedule day** { **friday** | **monday** | **saturday** | **sunday** | **thursday** | **tuesday** | **wednesday** } **start** *[HH:MM:SS]* **end** *[HH:MM:SS]*

**no wireless wps rogue ap rldp schedule day** { **friday** | **monday** | **saturday** | **sunday** | **thursday** | **tuesday** | **wednesday** } **start** *[HH:MM:SS]* **end** *[HH:MM:SS]*

## Syntax Description

| | |
|---|---|
| **day** {**friday** \| **monday** \| **saturday** \| **sunday** \| **thursday** \| **tuesday** \| **wednesday**} | Configures the day of the week when RLDP scheduling is to be done. |
| **start** *[HH:MM:SS]* | Configures the start time for RLDP schedule for the day. |
| **end** *[HH:MM:SS]* | Configures the end time for RLDP schedule for the day. |

## Command Default

None

## Command Modes

Global Configuration mode

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Amsterdam 16.12.1 | This command was introduced. |

## Usage Guidelines

None

### Example

The following example shows you how to configure the day of the week, when RLDP scheduling is to be done:

```
Device(config)# wireless wps rogue ap rldp schedule day friday start 10:10:10 end 15:15:15
```

# wireless wps rogue ap timeout

To configure the expiry time for rogue APs, in seconds, use the **wireless wps rogue ap timeout** command. Use the **no** form of this command to disable the configuration.

**wireless wps rogue ap timeout** *240-3600*

**no wireless wps rogue ap timeout** *240-3600*

## Syntax Description

| | |
|---|---|
| **rogue ap timeout** | Configures the expiry time for rogue APs, in seconds. |
| *240-3600* | Specifies the number of seconds before rogue entries are flushed. |

## Command Default

None

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.12.1 | This command was introduced. |

## Usage Guidelines

None

### Example

This example shows how to configure the expiry time for rogue APs, in seconds:

```
Device(config)# wireless wps rogue ap timeout 250
```

# wireless wps rogue auto-contain

To configure the auto contain level and to configure auto containment for monitor AP mode, use the **wireless wps rogue auto-contain** command. To disable the configuration, use the **no** form of this command.

**wireless wps rogue auto-contain** { **level** *1 - 4* | **monitor-ap-only** }

**no wireless wps rogue auto-contain** { **level** *1 - 4* | **monitor-ap-only** }

## Syntax Description

| | |
|---|---|
| **auto-contain** | Configures auto contain for rogue devices. |
| **level** | Configures auto contain levels. |
| *1 - 4* | Specifies the auto containment levels. |
| **monitor-ap-only** | Configures auto contain for monitor AP mode. |

## Command Default

None

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.12.1 | This command was introduced. |

## Usage Guidelines

None

### Example

This example shows how to configure the auto contain level and to configure auto containment for monitor AP mode:

```
Device(config)# wireless wps rogue auto-contain level 2
Device(config)# wireless wps rogue auto-contain monitor-ap-only
```

# wireless wps rogue client aaa

To configure the use of AAA or local database to detect valid MAC addresses of rogue clients, use the **wireless wps rogue client aaa** command. Use the **no** form of this command to disable the configuration.

**wireless wps rogue client aaa**

**no wireless wps rogue client aaa**

## Syntax Description

| | |
|---|---|
| **aaa** | Configures the use of AAA or local database to detect valid MAC addresses of rogue clients. |

## Command Default

None

## Command Modes

Global Configuration mode

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Amsterdam 16.12.1 | This command was introduced. |

## Usage Guidelines

None

### Example

The following example shows you how to configure the use of AAA or local database to detect valid MAC addresses of rogue clients:

```
Device(config)# wireless wps rogue client aaa
```

# wireless wps rogue client mse

To configure Mobility Services Engine (MSE) to detect valid MAC addresses of rogue clients, use the **wireless wps rogue client mse** command. Use the **no** form of this command to disable the configuration.

**wireless wps rogue client mse**

**no wireless wps rogue client mse**

## Syntax Description

| | |
|---|---|
| **mse** | Configures the MSE to detect valid MAC addresses of rogue clients. |

## Command Default

None

## Command Modes

Global Configuration mode

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Amsterdam 16.12.1 | This command was introduced. |

## Usage Guidelines

None

### Example

The following example shows you how to configure Mobility Services Engine (MSE) to detect valid MAC addresses of rogue clients:

```
Device(config)# wireless wps rogue client mse
```

# wireless wps rogue client client-threshold

To configure rogue client per a rogue AP SNMP trap threshold, use the **wireless wps rogue client client-threshold** command. To disable the configuration, use the **no** form of this command.

**wireless wps rogue client client-threshold** *0 - 256*

**no wireless wps rogue client client-threshold** *0 - 256*

## Syntax Description

| | |
|---|---|
| **rogue client** | Configures rogue clients. |
| **client-threshold** | Configures the rogue client per a rogue AP SNMP trap threshold. |
| *0 - 256* | Specifies the client threshold. |

## Command Default

None

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.12.1 | This command was introduced. |

## Usage Guidelines

None

### Example

This example shows how to configure rogue client per a rogue AP SNMP trap threshold:

```
Device(config)# wireless wps rogue ap timeout 250
```

# wireless wps rogue client notify-min-rssi

To configure the minimum RSSI notification threshold for rogue clients, use the **wireless wps rogue client notify-min-rssi** command. Use the **no** form of this command to disable the configuration.

**wireless wps rogue client notify-min-rssi** *-128 - -70*

**no wireless wps rogue client notify-min-rssi** *-128 - -70*

## Syntax Description

| | |
|---|---|
| **rogue clients** | Configures rogue clients. |
| **notify-min-rssi** | Configures the minimum RSSI notification threshold for rogue clients. |
| *-128 - -70* | Specifies the RSSI threshold in decibels. |

## Command Default

None

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.12.1 | This command was introduced. |

## Usage Guidelines

None

### Example

This example shows how to configure the minimum RSSI notification threshold for rogue clients:

```
Device(config)# wireless wps rogue client notify-min-rssi –125
```

# wireless wps rogue client notify-rssi-deviation

To configure the RSSI deviation notification threshold for rogue clients, use the **wireless wps rogue client notify-rssi-deviation** command. To disable the configuration, use the **no** form of this command.

**wireless wps rogue client notify-rssi-deviation** *0 - 10*

**no wireless wps rogue client notify-rssi-deviation** *0 - 10*

## Syntax Description

| | |
|---|---|
| **notify-rssi-deviation** | Configures the RSSI deviation notification threshold for rogue clients. |
| *0 - 10* | Specifies the RSSI threshold in decibels. |

## Command Default

None

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.12.1 | This command was introduced. |

## Usage Guidelines

None

### Example

This example shows how to configure the RSSI deviation notification threshold for rogue clients:

```
Device(config)# wireless wps rogue client notify-rssi-deviation 6
```

# wireless wps rogue detection

To configure various rouge 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## 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 notify-syslog

To enable syslog notification for rogue events, use the **wireless wps rogue notify-syslog** command.

**wireless wps rogue notify-syslog**

## Syntax Description

This command has no keywords or arguments.

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

### Example

This example shows how to enable syslog notification for rogue events:

```
Device# configure terminal
Device(config)# wireless wps rogue notify-syslog
```

# wireless wps rogue rule

To configure rogue classification rule, use the **wireless wps rogue rule** command.

**wireless wps rogue rule** *rule-name* **priority** *priority* {**classify** {**friendly** | **malicious**} | **condition** {**client-count number** | **duration** | **encryption** | **infrastructure** | **rssi** | **ssid**} | **default** | **exit** | **match** {**all** | **any**} | **no** | **shutdown**}

## Syntax Description

| | |
|---|---|
| **rule** *rule-name* | Specifies a rule name. |
| **priority** *priority* | Changes the priority of a specific rule and shifts others in the list accordingly. |
| **classify** | Specifies the classification of a rule. |
| **friendly** | Classifies a rule as friendly. |
| **malicious** | Classifies a rule as malicious. |
| **condition** {**client-count number** \| **duration** \| **encryption** \| **infrastructure** \| **rssi** \| **ssid**} | Specifies the conditions for a rule that the rogue access point must meet.<br>Type of the condition to be configured. The condition types are listed below:<br>• client-count—Requires that a minimum number of clients be associated to a rogue access point. The valid range is 1 to 10 (inclusive).<br>• duration—Requires that a rogue access point be detected for a minimum period of time. The valid range is 0 to 3600 seconds (inclusive).<br>• encryption—Requires that the advertised WLAN does not have encryption enabled.<br>• infrastructure—Requires the SSID to be known to the controller<br>• rssi—Requires that a rogue access point have a minimum RSSI value. The range is from –95 to –50 dBm (inclusive).<br>• ssid—Requires that a rogue access point have a specific SSID. |
| **default** | Sets the command to its default settings. |
| **exit** | Exits the sub-mode. |
| **match** {**all** \| **any**} | Configures matching criteria for a rule. Specifies whether a detected rogue access point must meet all or any of the conditions specified by the rule in order for the rule to be matched and the rogue access point to adopt the classification type of the rule. |
| **no** | Negates a command or set its defaults. |
| **shutdown** | Shuts down the system. |

## Command Default

None.

## Command Modes

Global configuration

### Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

### Usage Guidelines

None.

This example shows how to create a rule that can organize and display rogue access points as Friendly:

```
Device# configure terminal
Device(config)# wireless wps rogue rule ap1 priority 1
Device(config-rule)# classify friendly
Device(config)# end
```

# wireless wps rogue security-level

To configure the wireless WPS rogue detection security levels, use the **wireless wps rogue security-level** command. Use the **no** form of this command to disable the configuration.

**wireless wps rogue security-level** { **critical** | **custom** | **high** | **low** }

**no wireless wps rogue security-level** { **critical** | **custom** | **high** | **low** }

## Syntax Description

| | |
|---|---|
| **rogue security-level** | Configures the rogue detection security level. |
| **critical** | Specifies the rogue detection setup for highly sensitive deployments. |
| **custom** | Specifies the customizable security level. |
| **high** | Specifies the rogue detection setup for medium-scale deployments. |
| **low** | Specifies the basic rogue detection setup for small-scale deployments. |

## Command Default

None

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.12.1 | This command was introduced. |

## Usage Guidelines

None

### Example

This example shows how to configure the wireless WPS rogue detection security levels:

```
Device(config)# wireless wps rogue security-level critical
```

# wireless-default radius server

To configure multiple radius servers, use the **wireless-default radius server** command.

**wireless-default radius server** *IP* **key** *secret*

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

Using this utility, you can configure a maximum of ten radius servers.

### Example

This example shows how to configure multiple radius servers:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless-default radius server 9.2.58.90 key cisco123
Device(config)# end
```

# wlan policy

To map a policy profile to a WLAN profile, use the **wlan policy** command.

**wlan** *wlan-name* **policy** *policy-name*

## Syntax Description

| | |
|---|---|
| *wlan-name* | Name of the WLAN profile. |
| **policy** | Map a policy profile to the WLAN profile. |
| *policy-name* | Name of the policy profile. |

## Command Default

None

## Command Modes

config-policy-tag

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

# Show Commands

# show aaa dead-criteria radius

To verify the dead-server-detection information for a RADIUS server, use the **show aaa dead-criteria radius** command.

**show aaa dead-criteria radius** *ipaddr* **auth-port** *authport* **acct-port** *acctport*

## Syntax Description

| | |
|---|---|
| *ipaddr* | IP address. |
| *authport* | Authentication port. |
| *acctport* | Accounting port. |

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

## Usage Guidelines

The **show aaa dead-criteria radius** *ipaddr* command displays output only if default ports are used. For non-default ports, use the **show aaa dead-criteria radius** *ipaddr* **auth-port** *authport* **acct-port** *acctport* command.

### Example

The following example shows how to see the dead-server-detection information for a RADIUS server with non-default authorization and accounting ports:

```
Device# show aaa dead-criteria radius 4.4.4.4 auth-port 4444 acct-port 3333

RADIUS: No server group specified. Using radius
RADIUS Server Dead Criteria:
=============================
Server Details:
Address : 4.4.4.4
Auth Port : 4444
Acct Port : 3333
Server Group : radius
Dead Criteria Details:
Configured Retransmits : 3
Configured Timeout : 5
Estimated Outstanding Access Transactions: 0
Estimated Outstanding Accounting Transactions: 0
Dead Detect Time : 10s
Computed Retransmit Tries: 10
Statistics Gathered Since Last Successful Transaction
=====================================================
Max Computed Outstanding Transactions: 0
Max Computed Dead Detect Time: 0s
Max Computed Retransmits : 0
```

The following example shows how to see the dead-server-detection information for a RADIUS server using default ports:

```
Device# show aaa dead-criteria radius 9.3.13.37

RADIUS: No server group specified. Using radius
RADIUS Server Dead Criteria:
=============================
Server Details:
Address : 9.3.13.37
Auth Port : 1812
Acct Port : 1813
Server Group : radius
Dead Criteria Details:
Configured Retransmits : 3
Configured Timeout : 30
Estimated Outstanding Access Transactions: 1
Estimated Outstanding Accounting Transactions: 0
Dead Detect Time : 10s
Computed Retransmit Tries: 10
Statistics Gathered Since Last Successful Transaction
=====================================================
Max Computed Outstanding Transactions: 4
Max Computed Dead Detect Time: 48s
Max Computed Retransmits : 30
```

# show aaa servers

To display the status and number of packets that are sent to and received from all public and private authentication, authorization, and accounting (AAA) RADIUS servers as interpreted by the AAA Server MIB, use the **show aaa servers** command.

**show aaa servers [ private | public ]**

## Syntax Description

| | |
|---|---|
| **private** | (Optional) Displays private AAA servers only, which are also displayed by the AAA Server MIB. |
| **private** | (Optional) Displays public AAA servers only, which are also displayed by the AAA Server MIB. |

## Command Default

None

## Command Modes

Privileged EXEC(#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

## Usage Guidelines

Only RADIUS servers are supported by the **show aaa servers** command.

### Example

The following command displays information about packets sent and received for all AAA transaction types--authentication, authorization, and accounting.

```
Device# show aaa servers

RADIUS: id 2, priority 1, host 124.2.2.12, auth-port 1645, acct-port 1612, hostname rsim
     State: current UP, duration 20699s, previous duration 0s
     Dead: total time 0s, count 0
     Platform State from SMD: current UP, duration 20699s, previous duration 0s
     SMD Platform Dead: total time 0s, count 0
     Platform State from WNCD (1) : current UP
     Platform State from WNCD (2) : current UP
     Platform State from WNCD (3) : current UP
     Platform State from WNCD (4) : current UP
     Platform State from WNCD (5) : current UP
     Platform State from WNCD (6) : current UP
     Platform State from WNCD (7) : current UP
     Platform State from WNCD (8) : current UP, duration 964s, previous duration 0s
     Platform Dead: total time 0s, count 0UP
     Quarantined: No
.
.
.

     Elapsed time since counters last cleared: 5h44m
     Estimated Outstanding Access Transactions: 0
     Estimated Outstanding Accounting Transactions: 0
     Estimated Throttled Access Transactions: 0
     Estimated Throttled Accounting Transactions: 0
```

```
Maximum Throttled Transactions: access 0, accounting 0
Consecutive Response Failures: total 0
        SMD Platform : max 0, current 0 total 0
        WNCD Platform: max 0, current 0 total 0
        IOSD Platform : max 0, current 0 total 0
Consecutive Timeouts: total 0
        SMD Platform : max 0, current 0 total 0
        WNCD Platform: max 0, current 0 total 0
        IOSD Platform : max 0, current 0 total 0
Requests per minute past 24 hours:
        high - 5 hours, 44 minutes ago: 0
        low  - 5 hours, 44 minutes ago: 0
        average: 0
```

# show access-list

To display access control lists (ACLs) configured on the device, use the **show access-lists** command in privileged EXEC mode.

**show access-lists**[*namenumber* | **hardware counters** | **ipc**]

## Syntax Description

| | |
|---|---|
| *number* | (Optional) ACL number. The range is 1 to 2799. |
| *name* | (Optional) Name of the ACL. |
| **hardware counters** | (Optional) Displays the access list hardware counters. |
| **ipc** | (Optional) Display Interprocess Communication (IPC) protocol access-list configuration download information |

## Command Default

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.11.1 | This command was introduced. |

## Usage Guidelines

Though visible in the command-line help strings, the **rate-limit** keyword is not supported

The device supports only IP standard and extended access lists. Therefore, the allowed numbers are only 1 to 199 and 1300 to 2799.

This command also displays the MAC ACLs that are configured.

This is an example of output from the **show access-lists** command:

```
Device# show access-lists

Extended IP access list 103
    10 permit ip any any dscp af11
Extended IP access list ssm-range
    10 deny ip any 232.0.0.0 0.255.255.255
    20 permit ip any any
Extended MAC access list 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
```

```
    All  Drop And Log:              frame count: 0
    All  Bridge Only And Log:       frame count: 0
    All  Forwarded And Log:         frame count: 0
    All  IPv6 Drop:                 frame count: 0
    All  IPv6 Bridge Only:          frame count: 0
    All  IPv6 Forwarding To CPU:    frame count: 0
    All  IPv6 Forwarded:            frame count: 102
    All  IPv6 Drop And Log:         frame count: 0
    All  IPv6 Bridge Only And Log:  frame count: 0
    All  IPv6 Forwarded And Log:    frame count: 0

L3 ACL OUTPUT Statistics
    All  Drop:                      frame count: 0
    All  Bridge Only:               frame count: 0
    All  Forwarding To CPU:         frame count: 0
    All  Forwarded:                 frame count: 266050
    All  Drop And Log:              frame count: 0
    All  Bridge Only And Log:       frame count: 0
    All  Forwarded And Log:         frame count: 0
    All  IPv6 Drop:                 frame count: 0
    All  IPv6 Bridge Only:          frame count: 0
    All  IPv6 Forwarding To CPU:    frame count: 0
    All  IPv6 Forwarded:            frame count: 0
    All  IPv6 Drop And Log:         frame count: 0
    All  IPv6 Bridge Only And Log:  frame count: 0
    All  IPv6 Forwarded And Log:    frame count: 0
```

# show ap airtime-fairness summary

To view the ATF configuration summary of all radios, use the **show ap airtime-fairness summary** command.

**show ap airtime-fairness summary**

## Syntax Description

This command has no arguments.

## Command Default

None

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the ATF configuration summary of all radios:

```
Device# show ap airtime-fairness summary
```

# show ap 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

| | |
|---|---|
| *chassis-number* | Chassis number as either 1 or 2. |
| **active R0** | Active instance in Route-processor slot 0. |
| **standby R0** | Standby instance in Route-processor slot 0. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see the 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 dot11**{**24ghz** | **5ghz** |**dual-band**} *cisco_ap*

## Syntax Description

| | |
|---|---|
| **24ghz** | Specifies the 802.11b AP. |
| **5ghz** | Specifies the 802.11a AP. |
| **dual-band** | Specifies dual bands. |

## Command Default

None

## Usage Guidelines

The **show ap auto-rf command** output will not display neighbor AP names.

The following example shows how to display auto-RF information for an access point:

```
Device# show ap auto-rf dot11 24ghz AP1

###################################################################

Number of Slots                                   : 3
AP Name                                           : APA023.9FD8.EA22
MAC Address                                       : 40ce.24bf.8ca0
Ethernet MAC Address                              : a023.9fd8.ea22
  Slot ID                                         : 0
  Radio Type                                      : 802.11n - 2.4 GHz
  Current TX/RX Band                              : 2.4Ghz band
  Subband Type                                    : All
  Noise Information
    Noise Profile                                 : Passed
    Channel   1                                   :  -91 dBm
    Channel   2                                   :  -67 dBm
    Channel   3                                   :  -54 dBm
    Channel   4                                   :  -55 dBm
    Channel   5                                   :  -71 dBm
    Channel   6                                   :  -85 dBm
    Channel   7                                   :  -50 dBm
    Channel   8                                   :  -54 dBm
    Channel   9                                   :  -77 dBm
    Channel  10                                   :  -88 dBm
    Channel  11                                   :  -65 dBm
  Interference Information
    Interference Profile                          : Failed
    Channel   1                                   :  -47 dBm @ 21% busy
    Channel   2                                   :  -45 dBm @  2% busy
    Channel   3                                   : -128 dBm @  0% busy
    Channel   4                                   : -128 dBm @  0% busy
    Channel   5                                   :  -48 dBm @  2% busy
    Channel   6                                   :  -45 dBm @  2% busy
    Channel   7                                   :  -42 dBm @  3% busy
    Channel   8                                   : -128 dBm @  0% busy
    Channel   9                                   : -128 dBm @  0% busy
    Channel  10                                   :  -39 dBm @  3% busy
    Channel  11                                   :  -46 dBm @  3% busy
    Rogue Histogram (20)
      Channel   1                                 : 36
      Channel   2                                 :  0
      Channel   3                                 :  0
      Channel   4                                 :  1
      Channel   5                                 :  0
      Channel   6                                 : 11
      Channel   7                                 :  0
      Channel   8                                 :  1
      Channel   9                                 :  3
      Channel  10                                 :  0
      Channel  11                                 : 14
  Load Information
    Load Profile                                : Failed
    Receive Utilization                         : 0%
    Transmit Utilization                        : 0%
    Channel Utilization                         : 98%
    Attached Clients                            : 0 clients
  Coverage Information
    Coverage Profile                            : Passed
    Failed Clients                              : 0 clients
  Client Signal Strengths
    RSSI -100 dBm                               : 0 clients
    RSSI  -92 dBm                               : 0 clients
    RSSI  -84 dBm                               : 0 clients
    RSSI  -76 dBm                               : 0 clients
    RSSI  -68 dBm                               : 0 clients
    RSSI  -60 dBm                               : 0 clients
    RSSI  -52 dBm                               : 0 clients
  Client Signal to Noise Ratios
    SNR    0 dB                                 : 0 clients
    SNR    5 dB                                 : 0 clients
    SNR   10 dB                                 : 0 clients
    SNR   15 dB                                 : 0 clients
    SNR   20 dB                                 : 0 clients
    SNR   25 dB                                 : 0 clients
    SNR   30 dB                                 : 0 clients
    SNR   35 dB                                 : 0 clients
    SNR   40 dB                                 : 0 clients
    SNR   45 dB                                 : 0 clients
  Nearby APs
    AP d0ec.3572.b9a0 slot 0                    :  -23 dBm on ( 11, 20 MHz) (181.22.0.22)
    AP 0c75.bdb3.9000 slot 0                    :  -28 dBm on ( 11, 20 MHz) (181.21.0.21)
    AP a4b2.3980.3740 slot 0                    :  -28 dBm on (  1, 20 MHz) (181.21.0.21)
    AP d0ec.3576.8320 slot 0                    :  -33 dBm on ( 11, 20 MHz) (50.1.1.122)
    AP a0f8.49dc.9780 slot 0                    :  -34 dBm on (  1, 20 MHz) (9.9.57.94)
    AP a0f8.49dc.8260 slot 0                    :  -34 dBm on (  6, 20 MHz) (9.9.57.94)
    AP d0ec.3573.7c80 slot 0                   :  -36 dBm on (  6, 20 MHz) (192.185.183.44)

    AP 00b0.e192.9d20 slot 0                    :  -36 dBm on ( 11, 20 MHz) (9.9.42.47)
    AP a4b2.397f.41c0 slot 0                    :  -36 dBm on (  1, 20 MHz) (185.10.0.10)
    AP 2c5a.0fd5.b8c0 slot 0                    :  -36 dBm on (  6, 20 MHz) (9.7.97.51)
    AP a488.7351.4740 slot 0                    :  -36 dBm on ( 11, 20 MHz) (9.7.97.51)
    AP 10b3.d5e9.c8e0 slot 0                    :  -36 dBm on (  1, 20 MHz) (50.1.1.122)
    AP 0c75.bdb3.ab00 slot 0                    :  -37 dBm on (  6, 20 MHz) (185.10.0.10)
    AP 68ca.e451.5120 slot 0                    :  -37 dBm on (  1, 20 MHz) (9.4.155.15)
    AP a0f8.49dc.97a0 slot 0                    :  -37 dBm on ( 11, 20 MHz) (9.9.57.94)
    AP 188b.4501.7940 slot 0                    :  -38 dBm on ( 11, 20 MHz) (9.9.57.94)
    AP 002c.c88a.f8e0 slot 0                    :  -38 dBm on ( 11, 20 MHz) (9.9.50.55)
    AP 7069.5a78.4960 slot 0                    :  -38 dBm on ( 11, 20 MHz) (9.7.97.51)
    AP 3c41.0ea7.0880 slot 0                    :  -39 dBm on ( 11, 20 MHz) (185.10.0.10)
    AP a0f8.49dc.93a0 slot 0                    :  -39 dBm on (  6, 20 MHz) (9.9.57.94)
    AP f4db.e685.7360 slot 0                    :  -39 dBm on (  6, 20 MHz) (50.1.1.122)
    AP 7070.8bb4.4120 slot 0                    :  -40 dBm on ( 11, 20 MHz) (9.9.57.94)
    AP 707d.b93e.39e0 slot 0                    :  -40 dBm on (  1, 20 MHz) (4.4.4.1)
    AP 706d.150c.6860 slot 0                    :  -40 dBm on ( 11, 20 MHz) (50.1.1.122)
```

```
Radar Information
Channel Assignment Information via DCA
  Current Channel Average Energy                :  -50 dBm
  Previous Channel Average Energy               :  -50 dBm
  Channel Change Count                          : 9
  Last Channel Change Time                      : 02/14/2021 20:54:57
  Recommended Best Channel                      : 1
RF Parameter Recommendations
  Power Level                                   : 8
  RTS/CTS Threshold                             : 2347
  Fragmentation Threshold                       : 2346
  Antenna Pattern                               : 0
Persistent Interference Devices
Class Type                 Channel  DC (%%)  RSSI (dBm)  Last Update Time
-------------------------  -------  ------   ---------   ----------------
All third party trademarks are the property of their respective owners.
```

# show ap config

To display configuration settings for all access points that join the device, use the **show ap config** command.

**show ap config** {**general** | **global**}

## Syntax Description

| | |
|---|---|
| **ethernet** | Displays ethernet VLAN tagging information for all Cisco APs. |
| **general** | Displays common information for all Cisco APs. |
| **global** | Displays global settings for all Cisco APs. |

## Command Default

None

## Command Modes

Any command mode

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to display global syslog server settings:

```
Device# show ap config global

AP global system logging host                    : 255.255.255.255
```

# show ap 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-filechassis** *chassis-number <1-2>***active standby**

## Syntax Description

| | |
|---|---|
| **chassis** | Displays the chassis details. |
| *chassis-number* | Specifies the chassis number, either 1 or 2. |
| **active** | Specifies an active instance. |
| **standby** | Specifies a standby instance. |

## Command Default

None

## Command Modes

Any command mode

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to display the crash file generated by the access point:

```
Device# show ap crash-file
```

# show ap dot11

To view 802.11a or 802.11b 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** }

## Syntax Description

| | |
|---|---|
| **24ghz** | Specifies the 2.4-GHz band. |
| **5ghz** | Specifies the 5-GHz band. |
| **6ghz** | Specifies the 6-GHz band. |
| **channel** | Displays the automatic channel assignment configuration and statistics. |
| **coverage** | Displays the configuration and statistics for coverage hole detection. |
| **group** | Displays 802.11a or 802.11b Cisco radio RF grouping. |
| **load-info** | Displays channel utilization and client count information for all Cisco APs. |
| **logging** | Displays 802.11a or 802.11b RF event and performance logging. |
| **media-stream** | Display 802.11a or 802.11b Media Resource Reservation Control configurations. |
| **monitor** | Displays the 802.11a or 802.11b default Cisco radio monitoring. |
| **network** | Displays the 802.11a or 802.11b network configuration. |
| **profile** | Displays the 802.11a or 802.11b lightweight access point performance profiles. |
| **receiver** | Displays the configuration and statistics of the 802.11a or 802.11b receiver. |
| **service-policy** | Displays the Quality of Service (QoS) service policies for 802.11a or 802.11b radio for all Cisco access points. |
| **summary** | Displays the 802.11a or 802.11b Cisco lightweight access point name, channel, and transmit level summary. |
| **txpower** | Displays the 802.11a or 802.11b automatic transmit power assignment. |
| **ccx global** | Displays 802.11a or 802.11b Cisco Client eXtensions (CCX) information for all Cisco access points that are joined to the device. |

## Command Default

None

## Command Modes

Any command mode

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 Cisco IOS XE Gibraltar 16.12.2s | This command was introduced. |
| | The **load-info** parameter was added. |

This example shows how to display the automatic channel assignment configuration and statistics:

```
Device# show ap dot11 5ghz channel
Automatic Channel Assignment
  Channel Assignment Mode                    : AUTO
  Channel Update Interval                    : 12 Hours
  Anchor time (Hour of the day)              : 20
  Channel Update Contribution                : SNI.
  Channel Assignment Leader                  : web (9.9.9.2)
  Last Run                                   : 13105 seconds ago
  DCA Sensitivity Level                      : MEDIUM (15 dB)
  DCA 802.11n Channel Width                  : 40 Mhz
  Channel Energy Levels
      Minimum                                : unknown
      Average                                : unknown
      Maximum                                : unknown
  Channel Dwell Times
      Minimum                                : unknown
      Average                                : unknown
      Maximum                                : unknown
  802.11a 5 GHz Auto-RF Channel List
  Allowed Channel List                       : 36,40,44,48,52,56,60,64,149,153,1
57,161
  Unused Channel List                        : 100,104,108,112,116,132,136,140,1
65
  802.11a 4.9 GHz Auto-RF Channel List
  Allowed Channel List                       :
  Unused Channel List                        : 1,2,3,4,5,6,7,8,9,10,11,12,13,14,
15,16,17,18,19,20,21,22,23,24,25,26
  DCA Outdoor AP option                      : Disabled
```

This example shows how to display the statistics for coverage hole detection:

```
Device# show ap dot11 5ghz coverage
Coverage Hole Detection
  802.11a Coverage Hole Detection Mode          : Enabled
  802.11a Coverage Voice Packet Count           : 100 packet(s)
  802.11a Coverage Voice Packet Percentage      : 50 %
  802.11a Coverage Voice RSSI Threshold         : -80dBm
  802.11a Coverage Data Packet Count            : 50 packet(s)
  802.11a Coverage Data Packet Percentage       : 50 %
  802.11a Coverage Data RSSI Threshold          : -80dBm
  802.11a Global coverage exception level       : 25
  802.11a Global client minimum exception level   : 3 clients
```

This example shows how to display Cisco radio RF group settings:

```
Device# show ap dot11 5ghz group
Radio RF Grouping

  802.11a Group Mode                 : STATIC
  802.11a Group Update Interval      : 600 seconds
  802.11a Group Leader               : web (10.10.10.1)
  802.11a Group Member               : web(10.10.10.1)
                                       nb1(172.13.21.45) (*Unreachable)
  802.11a Last Run                   : 438 seconds ago


  Mobility Agents RF membership information
  ------------------------------------------------------------
  No of 802.11a MA RF-members : 0
```

This example shows how to display 802.11a RF event and performance logging:

```
Device# show ap dot11 5ghz logging
RF Event and Performance Logging

  Channel Update Logging              : Off
  Coverage Profile Logging            : Off
  Foreign Profile Logging             : Off
  Load Profile Logging                : Off
  Noise Profile Logging               : Off
  Performance Profile Logging         : Off
  TxPower Update Logging              : Off
```

This example shows how to display the 802.11a media stream configuration:

```
Device# show ap dot11 5ghz media-stream
Multicast-direct                 : Disabled
Best Effort                      : Disabled
Video Re-Direct                  : Disabled
Max Allowed Streams Per Radio      : Auto
Max Allowed Streams Per Client     : Auto
Max Video Bandwidth               : 0
Max Voice Bandwidth               : 75
Max Media Bandwidth               : 85
Min PHY Rate (Kbps)               : 6000
Max Retry Percentage              : 80
```

This example shows how to display the radio monitoring for the 802.11b network:

```
Device# show ap dot11 5ghz monitor
Default 802.11a AP monitoring

  802.11a Monitor Mode                          : Enabled
  802.11a Monitor Mode for Mesh AP Backhaul      : disabled
  802.11a Monitor Channels                      : Country channels
  802.11a RRM Neighbor Discover Type            : Transparent
  802.11a AP Coverage Interval                  : 180 seconds
  802.11a AP Load Interval                      : 60 seconds
  802.11a AP Noise Interval                     : 180 seconds
  802.11a AP Signal Strength Interval           : 60 seconds
```

This example shows how to display the global configuration and statistics of an 802.11a profile:

```
Device# show ap dot11 5ghz profile
Default 802.11a AP performance profiles
802.11a Global Interference threshold.............. 10%
802.11a Global noise threshold..................... -70 dBm
802.11a Global RF utilization threshold............ 80%
802.11a Global throughput threshold................ 1000000 bps
802.11a Global clients threshold................... 12 clients
802.11a Global coverage threshold.................. 12 dB
```

```
802.11a Global coverage exception level........... 80%
802.11a Global client minimum exception lev........ 3 clients
```

This example shows how to display the network configuration of an 802.11a profile:

```
Device# show ap dot11 5ghz network
802.11a Network : Enabled
11nSupport : Enabled
  802.11a Low Band : Enabled
  802.11a Mid Band : Enabled
  802.11a High Band : Enabled

802.11a Operational Rates
  802.11a 6M : Mandatory
  802.11a 9M : Supported
  802.11a 12M : Mandatory
  802.11a 18M : Supported
  802.11a 24M : Mandatory
  802.11a 36M : Supported
  802.11a 48M : Supported
  802.11a 54M : Supported
802.11n MCS Settings:
  MCS 0 : Supported
  MCS 1 : Supported
  MCS 2 : Supported
  MCS 3 : Supported
  MCS 4 : Supported
  MCS 5 : Supported
  MCS 6 : Supported
  MCS 7 : Supported
  MCS 8 : Supported
  MCS 9 : Supported
  MCS 10 : Supported
  MCS 11 : Supported
  MCS 12 : Supported
  MCS 13 : Supported
  MCS 14 : Supported
  MCS 15 : Supported
  MCS 16 : Supported
  MCS 17 : Supported
  MCS 18 : Supported
  MCS 19 : Supported
  MCS 20 : Supported
  MCS 21 : Supported
  MCS 22 : Supported
  MCS 23 : Supported
802.11n Status:
  A-MPDU Tx:
    Priority 0 : Enabled
    Priority 1 : Disabled
    Priority 2 : Disabled
    Priority 3 : Disabled
    Priority 4 : Enabled
    Priority 5 : Enabled
    Priority 6 : Disabled
    Priority 7 : Disabled
  A-MSDU Tx:
    Priority 0 : Enabled
    Priority 1 : Enabled
    Priority 2 : Enabled
    Priority 3 : Enabled
    Priority 4 : Enabled
    Priority 5 : Enabled
    Priority 6 : Disabled
    Priority 7 : Disabled
  Guard Interval : Any
  Rifs Rx : Enabled
Beacon Interval : 100
CF Pollable mandatory : Disabled
CF Poll Request Mandatory : Disabled
CFP Period : 4
CFP Maximum Duration : 60
Default Channel : 36
Default Tx Power Level : 1
DTPC Status : Enabled
Fragmentation Threshold : 2346
Pico-Cell Status : Disabled
Pico-Cell-V2 Status : Disabled
TI Threshold : 0
Legacy Tx Beamforming setting : Disabled
Traffic Stream Metrics Status : Disabled
Expedited BW Request Status : Disabled
EDCA profile type check : default-wmm
Call Admision 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 bandwith sample-size : 20
Video AC
  Video AC - Admission control (ACM) : Disabled
  Video max RF bandwidth : Infinite
  Video reserved roaming bandwidth : 0
```

This example shows how to display the global configuration and statistics of an 802.11a profile:

```
Device# show ap dot11 5ghz receiver
Default 802.11a AP performance profiles
802.11a Global Interference threshold.............. 10%
802.11a Global noise threshold..................... -70 dBm
802.11a Global RF utilization threshold............ 80%
802.11a Global throughput threshold................ 1000000 bps
802.11a Global clients threshold................... 12 clients
802.11a Global coverage threshold.................. 12 dB
802.11a Global coverage exception level............ 80%
802.11a Global client minimum exception lev........ 3 clients
```

This example shows how to display the global configuration and statistics of an 802.11a profile:

```
Device# show ap dot11 5ghz service-policy
```

This example shows how to display a summary of the 802.11b access point settings:

```
Device# show ap dot11 5ghz summary
AP Name MAC Address       Admin State Operation State Channel TxPower
------- ----------------- ----------- --------------- ------- -------
CJ-1240 00:21:1b:ea:36:60 ENABLED     UP              161     1( )
CJ-1130 00:1f:ca:cf:b6:60 ENABLED     UP              56*     1(*)
```

This example shows how to display the configuration and statistics of the 802.11a transmit power cost:

```
Device# show ap dot11 5ghz txpower
Automatic Transmit Power Assignment

Transmit Power Assignment Mode          : AUTO
Transmit Power Update Interval          : 600 seconds
Transmit Power Threshold                : -70 dBm
Transmit Power Neighbor Count           : 3 APs
Min Transmit Power                      : -10 dBm
Max Transmit Power                      : 30 dBm
Transmit Power Update Contribution      : SNI.
Transmit Power Assignment Leader        : web (10.10.10.1)
Last Run                                : 437 seconds ago
```

This example shows how to display the configuration and statistics of the 802.11a transmit power cost:

```
Device# show ap dot11 5ghz ccx global
 802.11a Client Beacon Measurements:
     disabled
```

# show ap dot11

To display 802.11 band parameters, use the **show ap dot11** command.

**show ap dot11** {**24ghz** | **5ghz**} {**media-stream rrc** | **network** | **profile** | **summary**}

## Syntax Description

| | |
|---|---|
| **media-stream rrc** | Displays Media Stream configurations. |
| **network** | Shows network configuration. |
| **profile** | Shows profiling information for all Cisco APs. |
| **summary** | Shows configuration and statistics of 802.11b and 802.11a Cisco APs. |

## Command Default

None

## Command Modes

User EXEC command mode or Privileged EXEC command mode

## Usage Guidelines

None.

The following is a sample output of the **show ap dot11 24ghz media-stream rrc** command.

```
Device#show ap dot11 24ghz media-stream rrc

Multicast-direct                 : Disabled
Best Effort                      : Disabled
Video Re-Direct                  : Disabled
Max Allowed Streams Per Radio      : Auto
Max Allowed Streams Per Client     : Auto
Max Video Bandwidth               : 0
Max Voice Bandwidth               : 75
Max Media Bandwidth               : 85
Min PHY Rate (Kbps)               : 6000
Max Retry Percentage              : 80
```

# show ap dot11 24ghz

To display the 2.4 GHz RRM parameters, use the **show ap dot11 24ghz** command.

**show ap dot11 24ghz** {**ccx** | **channel** | **coverage** | **group** | **l2roam** | **logging** | **monitor** | **profile** | **receiver** | **summary** | **txpower**}

## Syntax Description

| | |
|---|---|
| **ccx** | Displays the 802.11b CCX information for all Cisco APs. |
| **channel** | Displays the configuration and statistics of the 802.11b channel assignment. |
| **coverage** | Displays the configuration and statistics of the 802.11b coverage. |
| **group** | Displays the configuration and statistics of the 802.11b grouping. |
| **l2roam** | Displays 802.11b l2roam information. |
| **logging** | Displays the configuration and statistics of the 802.11b event logging. |
| **monitor** | Displays the configuration and statistics of the 802.11b monitoring. |
| **profile** | Displays 802.11b profiling information for all Cisco APs. |
| **receiver** | Displays the configuration and statistics of the 802.11b receiver. |
| **summary** | Displays the configuration and statistics of the 802.11b Cisco APs. |
| **txpower** | Displays the configuration and statistics of the 802.11b transmit power control. |

## Command Default

None.

## Command Modes

Global configuration.

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

None.

This example shows how to display configuration and statistics of the 802.11b coverage.

```
Device#show ap dot11 24ghz coverage

Coverage Hole Detection
  802.11b Coverage Hole Detection Mode              : Enabled
  802.11b Coverage Voice Packet Count               : 100 packet(s)
  802.11b Coverage Voice Packet Percentage          : 50%
  802.11b Coverage Voice RSSI Threshold             : -80 dBm
  802.11b Coverage Data Packet Count                : 50 packet(s)
  802.11b Coverage Data Packet Percentage           : 50%
  802.11b Coverage Data RSSI Threshold              : -80 dBm
```

```
802.11b Global coverage exception level          : 25 %
802.11b Global client minimum exception level    : 3 clients
```

# show ap dot11 24ghz SI config

To see the spectrum intelligence (SI) configuration details for the 2.4-GHz band, use the **show ap dot11 24ghz SI config** command.

**show ap dot11 24ghz SI config** [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

## Syntax Description

| | |
|---|---|
| *chassis-number* | Chassis number as either 1 or 2. |
| **active R0** | Active instance of the configuration in Route-processor slot 0. |
| **standby R0** | Standby instance of the configuration in Route-processor slot 0. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see the SI configuration details for the 2.4-GHz band:

```
Device# show ap dot11 24ghz SI config chassis 1 R0
```

# show ap dot11 24ghz SI device type

To see the spectrum intelligence (SI) interferers of different types for the 2.4-GHz band, use the **show ap dot11 24ghz SI device type** command.

**show ap dot11 24ghz SI device type** {**cont_tx** | **mw_oven** | **si_fhss**} [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

## Syntax Description

| | |
|---|---|
| **cont_tx** | SI interferers of type Continuous transmitter for the 2.4-GHz band. |
| **mw_oven** | SI interferers of type microwave oven for the 2.4-GHz band. |
| **si_fhss** | SI interferers of type Frequency Hopping Spread Spectrum for the 2.4-GHz band. |
| *chassis-number* | Enter the chassis number as either 1 or 2. |
| **active R0** | Active instance of the configuration in Route-processor slot 0. |
| **standby R0** | Standby instance of the configuration in Route-processor slot 0. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

None.

This example shows configuration and statistics of 802.11a channel assignment.

```
Device#show ap dot11 5ghz channel

Automatic Channel Assignment
  Channel Assignment Mode                        : AUTO
  Channel Update Interval                        : 12 Hours
  Anchor time (Hour of the day)                  : 20
  Channel Update Contribution                    : SNI..
  Channel Assignment Leader                      : web (9.9.9.2)
  Last Run                                       : 16534 seconds ago
  DCA Sensitivity Level                          : MEDIUM (15 dB)
  DCA 802.11n Channel Width                      : 40 Mhz
```

```
Channel Energy Levels
    Minimum                              : unknown
    Average                              : unknown
    Maximum                              : unknown
Channel Dwell Times
    Minimum                              : unknown
    Average                              : unknown
    Maximum                              : unknown
802.11a 5 GHz Auto-RF Channel List
Allowed Channel List                     : 36,40,44,48,52,56,60,64,149,153,1

               57,161
Unused Channel List                      : 100,104,108,112,116,132,136,140,1

               65
802.11a 4.9 GHz Auto-RF Channel List
Allowed Channel List                     :
Unused Channel List                      : 1,2,3,4,5,6,7,8,9,10,11,12,13,14,

               15,16,17,18,19,20,21,22,23,24,25,26
DCA Outdoor AP option                    : Disabled
```

# show ap dot11 24ghz cleanair air-quality

To display the air-quality summary information and air-quality worst information for the 802.11 networks, use the **show ap dot11 cleanair** command.

**show ap dot11** {**24ghz** | **5ghz** | **dual-band**} **cleanair** {**air-quality** | **config** | **device** | **summary**}

## Syntax Description

| | |
|---|---|
| **24ghz** | Displays the 2.4 GHz band. |
| **5ghz** | Displays the 5 GHz band. |
| **dual-band** | Displays 802.11 dual-band radios. |
| **cleanair** | Displays cleanair configurations. |
| **air-quality** | Displays the Cleanair Air-Quality (AQ) data for 2.4GHz band. |
| **device** | Displays the CleanAir Interferers of device for 2.4GHz band. |
| **config** | Displays CleanAir Configuration for 2.4GHz band. |
| **summary** | Displays cleanair configurations for all 802.11a Cisco APs. |

## Command Default

None

## Command Modes

Any command mode

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to display the worst air-quality information for the 5 GHz band:

```
Device# show ap dot11 5ghz cleanair air-quality worst

AQ = Air Quality
DFS = Dynamic Frequency Selection
AP Name      Channel Avg AQ Min AQ Interferers DFS
------------ ------- ------ ------ ----------- -----
CISCO_AP3500 36      95     70     0           40
```

This example shows how to display the worst air-quality information for the 2.4 GHz band:

```
Device# show ap dot11 24ghz cleanair air-quality worst

AQ = Air Quality
DFS = Dynamic Frequency Selection
AP Name      Channel Avg AQ Min AQ Interferers DFS
------------ ------- ------ ------ ----------- -----
CISCO_AP3500 1       83     57     3           5
```

# show ap dot11 24ghz cleanair air-quality

To display the air-quality summary information and air-quality worst information for the 802.11 networks, use the **show ap dot11 cleanair air-quality** command.

**show ap dot11** {**24ghz** | **5ghz**} **cleanair air-quality** {**summary** | **worst**}

## Syntax Description

| | |
|---|---|
| **24ghz** | Displays the 2.4 GHz band. |
| **5ghz** | Displays the 5 GHz band. |
| **summary** | Displays a summary of 802.11 radio band air-quality information. |
| **worst** | Displays the worst air-quality information for 802.11 networks. |

## Command Default

None

## Command Modes

Any command mode

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to display the worst air-quality information for the 5 GHz band:

```
Device# show ap dot11 5ghz cleanair air-quality worst

AQ = Air Quality
DFS = Dynamic Frequency Selection
AP Name      Channel Avg AQ Min AQ Interferers DFS
------------ ------- ------ ------ ----------- -----
CISCO_AP3500 36      95     70     0           40
```

This example shows how to display the worst air-quality information for the 2.4 GHz band:

```
Device# show ap dot11 24ghz cleanair air-quality worst

AQ = Air Quality
DFS = Dynamic Frequency Selection
AP Name      Channel Avg AQ Min AQ Interferers DFS
------------ ------- ------ ------ ----------- -----
CISCO_AP3500 1       83     57     3           5
```

# show ap dot11 cleanair config

To display the CleanAir configuration for the 802.11 networks, use the **show ap dot11 cleanair config** command.

**show ap dot11** {**24ghz** | **5ghz**} **cleanair config**

### Syntax Description

| | |
|---|---|
| **24ghz** | Displays the 2.4 GHz band. |
| **5ghz** | Displays the 5 GHz band. |

### Command Default

None

### Command Modes

Any command mode

### Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to display the CleanAir configuration for the 2.4 GHz band:

```
Device# show ap dot11 24ghz cleanair config
Clean Air Solution............................... : Disabled
Air Quality Settings:
    Air Quality Reporting........................ : Disabled
    Air Quality Reporting Period (min)........... : 15
    Air Quality Alarms........................... : Enabled
    Air Quality Alarm Threshold.................. : 10
Interference Device Settings:
    Interference Device Reporting................ : Enabled
        Bluetooth Link........................... : Enabled
        Microwave Oven........................... : Enabled
        802.11 FH................................ : Enabled
        Bluetooth Discovery...................... : Enabled
        TDD Transmitter.......................... : Enabled
        Jammer................................... : Enabled
        Continuous Transmitter................... : Enabled
        DECT-like Phone.......................... : Enabled
        Video Camera............................. : Enabled
        802.15.4................................. : Enabled
        WiFi Inverted............................ : Enabled
        WiFi Invalid Channel..................... : Enabled
        SuperAG.................................. : Enabled
        Canopy................................... : Enabled
        Microsoft Device......................... : Enabled
        WiMax Mobile............................. : Enabled
        WiMax Fixed.............................. : Enabled
    Interference Device Types Triggering Alarms:
        Bluetooth Link........................... : Disabled
        Microwave Oven........................... : Disabled
        802.11 FH................................ : Disabled
        Bluetooth Discovery...................... : Disabled
        TDD Transmitter.......................... : Disabled
        Jammer................................... : Disabled
        Continuous Transmitter................... : Disabled
        DECT-like Phone.......................... : Disabled
```

```
            Video Camera............................. : Disabled
            802.15.4................................. : Disabled
            WiFi Inverted............................ : Enabled
            WiFi Invalid Channel..................... : Enabled
            SuperAG.................................. : Disabled
            Canopy................................... : Disabled
            Microsoft Device......................... : Disabled
            WiMax Mobile............................. : Disabled
            WiMax Fixed.............................. : Disabled
        Interference Device Alarms................... : Enabled
    Additional Clean Air Settings:
        CleanAir Event-driven RRM State.............. : Disabled
        CleanAir Driven RRM Sensitivity.............. : LOW
        CleanAir Persistent Devices state............ : Disabled
```

# show ap dot11 cleanair summary

To view CleanAir configurations for all 802.11a Cisco APs, use the **show ap dot11 cleanair summary** command.

**show ap dot11** {**24ghz** | **5ghz**} **cleanair summary**

### Syntax Description

| | |
|---|---|
| **24ghz** | Specifies the 2.4-GHz band |
| **5ghz** | Specifies the 5-GHz band |
| **cleanair summary** | Summary of CleanAir configurations for all 802.11a Cisco APs |

### Command Default

None

### Command Modes

Any command mode

### Command History

| Release | Modification |
|---|---|
| | This command was introduced. |

# show ap dot11 dual-band summary

To view a brief summary of access points with dual-band radios, use the **show ap dot11 dual-band summary** command.

**show ap dot11 dual-band summary**

### Syntax Description

This command has no keywords or arguments.

### Command Default

None

### Command Modes

Privileged EXEC

### Command History

### Example

The following example shows how to view brief summary of tag names:

```
Device# show ap dot11 dual-band summary
```

# show ap environment

To see the AP environment information of all APs, use the **show ap environment** command.

**show ap environment** [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

## Syntax Description

| | |
|---|---|
| *chassis-number* | Enter the chassis number as either 1 or 2. |
| **active R0** | Active instance of the AP filters in Route-processor slot 0. |
| **standby R0** | Standby instance of the AP filters in Route-processor slot 0. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see the AP environment information:

```
Device# show ap environment
```

# show ap filters active

To see the details of active AP filters, use the **show ap filters active** command.

**show ap filters active** [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

## Syntax Description

| | |
|---|---|
| *chassis-number* | Chassis number as either 1 or 2. |
| **active R0** | Active instance of the active AP filters in Route-processor slot 0. |
| **standby R0** | Standby instance of the active AP filters in Route-processor slot 0. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see the details of the active AP filters for the active instance:

```
Device# show ap filters active chassis active R0
```

# show ap filters all

To see the details of all AP filters, use the **show ap filters all** command.

**show ap filters all** [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

## Syntax Description

| | |
|---|---|
| *chassis-number* | Enter the chassis number as either 1 or 2. |
| **active R0** | Active instance of the AP filters in Route-processor slot 0. |
| **standby R0** | Standby instance of the AP filters in Route-processor slot 0. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see the details of all the AP filters for the active instance:

```
Device# show ap filters all chassis active R0
```

# show ap fra

To see the flexible radio assignment (FRA) configurations in APs, use the **show ap fra** command.

**show ap fra** [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

## Syntax Description

| | |
|---|---|
| *chassis-number* | Chassis number as either 1 or 2. |
| **active R0** | Active instance in Route-processor slot 0. |
| **standby R0** | Standby instance in Route-processor slot 0. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see the FRA configurations in APs:

```
Device# show ap fra
```

# show ap gps location

To see the GPS location of all APs, use the **show ap gps location** command.

**show ap gps location** [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

## Syntax Description

| | |
|---|---|
| *chassis-number* | Enter the chassis number as either 1 or 2. |
| **active R0** | Active instance of the AP filters in Route-processor slot 0. |
| **standby R0** | Standby instance of the AP filters in Route-processor slot 0. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see the GPS location of all APs:

```
Device# show ap gps location
```

# show ap group hyperlocation

To view a summary or detailed information of Hyperlocation configuration for an AP group, use the **show ap group** *ap-group-name* **hyperlocation** command.

**show ap group hyperlocation** {**summary** | **detail**}

## Syntax Description

| | |
|---|---|
| **summary** | Shows the overall configuration values (AP group specific) and operational status and parameters for the AP group. |
| **detail** | Shows both overall (AP group specific) and per-AP configuration values and operational status for the AP group. The APs listed are only those that belong to the AP group. |

## Command Modes

User EXEC

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Denali 16.3.1 | This command was introduced. |

This example shows how to view a summary of Hyperlocation configuration for an AP group:

```
Device# show ap group my-ap-group hyperlocation summary

Site Name: my-ap-group
Site Description: This is an AP group
Hyperlocation operational status: Up
Reason: N/A
Hyperlocation NTP server: 9.0.0.4
Hyperlocation admin status: Enabled
Hyperlocation detection threshold: -100 dBm
Hyperlocation trigger threshold: 11
Hyperlocation reset threshold: 9
```

**Note** For Hyperlocation to be operational, the following conditions must be met:

- At least one Cisco CMX with Hyperlocation enabled
- Hyperlocation admin state operational
- Either AP NTP or IOS NTP configured

This example shows how to view detailed information about Hyperlocation configuration for an AP group:

```
Device# show ap group my-ap-group hyperlocation detail

Site Name: my-ap-group
Site Description: This is an AP group
Hyperlocation operational status: Up
Reason: N/A
Hyperlocation NTP server: 9.0.0.4
Hyperlocation admin status: Enabled
Hyperlocation detection threshold: -100 dBm
Hyperlocation trigger threshold: 11
Hyperlocation reset threshold: 9

Values for APs in all AP Groups:

AP Name                 Radio MAC        Method    Hyperlocation
-----------------------------------------------------------------
APf07f.0635.2d40        f07f.0676.3b89   WSM       Enabled
APf4cf.e272.4ed0        f4cf.e223.ba31   Local     Enabled
```

# show history channel interface dot11Radio all

To check channel change or trigger reason and history, use the **show history channel interface dot11Radio all** command.

**show history channel interface dot11Radio all**

## Syntax Description

This command has no keywords or arguments.

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Amsterdam 17.2.1 | This command was introduced. |

## Examples

This example shows how to check channel change or trigger reason and history:

```
Device# show history channel interface dot11Radio all

               Timestamp Slot Client count Channel Trigger
Fri May 31 12:57:04 2019    0            0      11 RRM-DCA
Fri May 31 13:10:02 2019    0            0       1 RRM-DCA
Fri May 31 12:57:04 2019    1            0      60  Manual
Fri May 31 13:00:16 2019    1            0     149     DFS
```

# show ap hyperlocation

To view a summary or detailed information about the hyperlocation configuration, use the **show ap hyperlocation** command.

**show ap hyperlocation** {**summary** | **detail**}

## Syntax Description

| | |
|---|---|
| **summary** | Shows the overall configuration and operational values. |
| **detail** | Shows the overall configuration and operation values as well as detailed information about each AP. |

## Command Default

None

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Denali 16.2.1 | This command was introduced. |
| Cisco IOS XE Denali 16.3.1 | This command was modified. The **ble-beacon** keyword was added. |

## Usage Guidelines

For hyperlocation to be operational, the following conditions must be met:

- At least one Cisco Connected Mobile Experiences (CMX) must be present with hyperlocation enabled.
- The hyperlocation admin state should be operational.
- Either AP Network Time Protocol (NTP) or IOS NTP should be configured.

### Example

This example shows how to view a summary of the hyperlocation configuration:

```
Device# show ap hyperlocation summary

Hyperlocation operational status: Up
Hyperlocation NTP server currently used: 9.0.0.4
Hyperlocation admin status: Enabled
Hyperlocation detection threshold: -100 dBm
Hyperlocation trigger threshold: 10
Hyperlocation reset threshold: 8
```

This example shows how to view detailed information about hyperlocation configuration:

```
Device# show ap hyperlocation detail

Hyperlocation operational status: Up
Hyperlocation NTP server currently used: 9.0.0.4
Hyperlocation admin status: Enabled
Hyperlocation detection threshold: -100 dBm
Hyperlocation trigger threshold: 10
Hyperlocation reset threshold: 8
```

```
AP Name                 Radio MAC        Method    Hyperlocation
----------------------------------------------------------------
AP84b8.0252.b930        84b8.0216.c721   HALO      Enabled
AP84b8.0265.5540        84b8.0243.8796   WSM       Enabled
APf07f.0635.2d40        f07f.0676.3b89   WSM       Enabled
APf4cf.e272.4ed0        f4cf.e223.ba31   HALO      Enabled
```

# show ap hyperlocation cmx summary

To see a summary of CMX informaiton with Hyperlocation enabled, use the **show ap hyperlocation cmx summary** command.

**show ap hyperlocation cmx summary** [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

## Syntax Description

| | |
|---|---|
| *chassis-number* | Enter the chassis number as either 1 or 2. |
| **active R0** | Active instance of the AP filters in Route-processor slot 0. |
| **standby R0** | Standby instance of the AP filters in Route-processor slot 0. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see a summary of CMX informaiton with Hyperlocation enabled:

```
Device# show ap hyperlocation cmx summary
```

# show ap image

To display the images present on Cisco lightweight access points, use the **show ap image** command.

**show ap image**

## Syntax Description

This command has no keywords and arguments.

## Command Default

None

## Command Modes

Any command mode

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to display images on the access points:

```
Device# show ap image
```

# show ap link-encryption

To display the link encryption status, use the **show ap link-encryption** command.

**show ap link-encryption**[**chassis** | {*chassis-number* | **active** | **standby**} | **R0**]

## Syntax Description

| | |
|---|---|
| *chassis-number* | Chassis number as either 1 or 2. |
| **active R0** | Active instance in Route-processor slot 0. |
| **standby R0** | Standby instance in Route-processor slot 0. |

## Command Default

None

## Command Modes

Any command mode

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example show how to display the link-encryption status:

```
Device# show Cisco IOS XE Gibraltar 16.12.2s link-encryption
```

# show ap primary list

To see the AP primary list, use the **show ap primary list** command.

**show ap primary list** [ **chassis** | { *chassis-number* | **active** | **standby** } | **R0** ]

## Syntax Description

|  |  |
|---|---|
| *chassis-number* | Chassis number as either 1 or 2. |
| **active R0** | Active instance in Route-processor slot 0. |
| **standby R0** | Standby instance in Route-processor slot 0. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see the AP primary list:

```
Device# show ap primary list
```

# show ap monitor-mode summary

To display the current channel-optimized monitor mode settings, use the **show ap monitor-mode summary** command.

**show ap monitor-mode summary**

## Syntax Description

This command has no keywords and arguments.

## Command Default

None

## Command Modes

Any command mode

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to display current channel-optimized monitor mode settings:

```
Device# show ap monitor-mode summary

AP Name Ethernet MAC      Status   Scanning Channel List
------- -------------     -------- -------- ----------------
AP_004  xx:xx:xx:xx:xx:xx Tracking 1,6,11,  4
```

# show ap multicast mom (multicast over multicast)

To confirm if the APs receive multicast to multicast (mom) traffic sent by the controller, using CAPWAP multicast group, use the **show ap multicast mom** command.

## Syntax Description

This command has no keywords and arguments.

## Command Default

None

## Command Modes

Previleged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Amsterdam 17.2 | This command was introduced. |

This example shows how to confirm if the APs receive multicast to multicast traffic sent by the controller using CAPWAP multicast group:

```
Device# show ap multicast mom

AP Name                    MOM-IP     TYPE MOM- STATUS
------------------------------------------------------
SS-E-1                     IPv4             Up
SS-E-2                     IPv4             Up
9130E-r3-sw2-g1012         IPv4             Up
9115i-r3-sw2-te1-0-38      IPv4             Up
AP9120-r3-sw3-Gi1-0-46     IPv4             Up
ap3800i-r2-sw1-te2-0-2     IPv4             Up
```

# show ap name auto-rf

To display the auto-RF settings for a Cisco lightweight access point, use the **show ap name auto-rf** command.

**show ap name** *ap-name* **auto-rf dot11** {**24ghz** | **5ghz** | **dual-band**}

## Syntax Description

| | |
|---|---|
| *ap-name* | Name of the Cisco lightweight access point. |
| **24ghz** | Displays the 2.4 GHz band. |
| **5ghz** | Displays the 5 GHz band. |
| **dual-band** | Displays dual band. |

## Command Default

None

## Command Modes

Privileged EXEC.

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to display auto-RF information for an access point:

```
Device# show ap name AP01 auto-rf dot11 24ghz

Number of Slots                                        : 2
AP Name                                                : TSIM_AP-1
MAC Address                                            : 0000.2000.02f0
Slot ID                                                : 0
Radio Type                                             : 802.11b/g
Subband Type                                           : All

Noise Information
  Noise Profile                                        : Failed
  Channel   1                                           :   24 dBm
  Channel   2                                           :   48 dBm
  Channel   3                                           :   72 dBm
  Channel   4                                           :   96 dBm
  Channel   5                                           :  120 dBm
  Channel   6                                           : -112 dBm
  Channel   7                                           :  -88 dBm
  Channel   8                                           :  -64 dBm
  Channel   9                                           :  -40 dBm
  Channel  10                                           :  -16 dBm
  Channel  11                                           :    8 dBm

Interference Information
  Interference Profile                                 : Passed
  Channel   1                                           : -128 dBm @  0% busy
  Channel   2                                           :  -71 dBm @  1% busy
  Channel   3                                           :  -72 dBm @  1% busy
  Channel   4                                           :  -73 dBm @  2% busy
  Channel   5                                           :  -74 dBm @  3% busy
  Channel   6                                           :  -75 dBm @  4% busy
  Channel   7                                           :  -76 dBm @  5% busy
  Channel   8                                     :  -77 dBm @  5% busy
  Channel   9                                     :  -78 dBm @  6% busy
  Channel  10                                     :  -79 dBm @  7% busy
  Channel  11                                     :  -80 dBm @  8% busy

Rogue Histogram (20/40_ABOVE/40_BELOW)
    Channel  36                                   : 27/ 4/ 0
    Channel  40                                   : 13/ 0/ 0
    Channel  44                                   :  5/ 0/ 0
    Channel  48                                   :  6/ 0/ 1
    Channel  52                                   :  4/ 0/ 0
    Channel  56                                   :  5/ 0/ 0
    Channel  60                                   :  1/ 3/ 0
    Channel  64                                   :  3/ 0/ 0
    Channel 100                                   :  0/ 0/ 0
    Channel 104                                   :  0/ 0/ 0
    Channel 108                                   :  0/ 1/ 0

Load Information
  Load Profile                                   : Passed
  Receive Utilization                            : 10%
  Transmit Utilization                           : 20%
  Channel Utilization                            : 50%
  Attached Clients                               : 0 clients

Coverage Information
  Coverage Profile                               : Passed
  Failed Clients                                 : 0 clients

Client Signal Strengths
  RSSI -100 dBm                                  : 0 clients
  RSSI  -92 dBm                                  : 0 clients
  RSSI  -84 dBm                                  : 0 clients
  RSSI  -76 dBm                                  : 0 clients
  RSSI  -68 dBm                                  : 0 clients
  RSSI  -60 dBm                                  : 0 clients
  RSSI  -52 dBm                                  : 0 clients

Client Signal to Noise Ratios
  SNR    0 dB                                    : 0 clients
  SNR    5 dB                                    : 0 clients
  SNR   10 dB                                    : 0 clients
  SNR   15 dB                                    : 0 clients
  SNR   20 dB                                    : 0 clients
  SNR   25 dB                                    : 0 clients
  SNR   30 dB                                    : 0 clients
  SNR   35 dB                                    : 0 clients
  SNR   40 dB                                    : 0 clients
  SNR   45 dB                                    : 0 clients

Nearby APs
  AP 0000.2000.0300 slot 0                       : -68 dBm on  11 (10.10.10.1)
  AP 0000.2000.0400 slot 0                       : -68 dBm on  11 (10.10.10.1)
  AP 0000.2000.0600 slot 0                       : -68 dBm on  11 (10.10.10.1)

Radar Information

Channel Assignment Information
  Current Channel Average Energy                 : 0 dBm
  Previous Channel Average Energy                : 0 dBm
  Channel Change Count                           : 0
  Last Channel Change Time                       : Wed Oct 17 08:13:36 2012
  Recommended Best Channel                       : 11
```

```
RF Parameter Recommendations
  Power Level                                      : 1
  RTS/CTS Threshold                                : 2347
  Fragmentation Threshold                          : 2346
  Antenna Pattern                                  : 0

Persistent Interference Devices
```

# show ap name ble detail

To display BLE management details, use the **show ap name ble detail** command.

**show ap name** *ap-name* **ble detail**

## Syntax Description

| | |
|---|---|
| *ap-name* | Specifies the name of the AP. |

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Amsterdam 17.3.1 | This command was introduced. |

## Usage Guidelines

None

### Example

The following example shows how to display the BLE management details:

```
Device(config)# show ap name ap-name ble detail
```

# show ap name cablemodem

To see cable modem information of an AP, use the **show ap name** *ap-name* **cablemodem** command.

**show ap name** *ap-name* **cablemodem** [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

## Syntax Description

| | |
|---|---|
| *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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see cable modem information of an AP:

```
Device# show ap name my-ap cablemodem
```

# show ap name config

To display common information and Ethernet VLAN tagging information for a specific Cisco lightweight access point, use the **show ap name config** command.

**show ap name** *ap-name* **config** {**ethernet** | **general**}

## Syntax Description

| | |
|---|---|
| *ap-name* | Name of the Cisco lightweight access point. |
| **ethernet** | Displays Ethernet tagging configuration information for an access point. |
| **general** | Displays common information for an access point. |

## Command Default

None

## Command Modes

Any command mode

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to display Ethernet tagging information for an access point:

```
Device# show ap name AP01 config ethernet

VLAN Tagging Information for AP01
```

This example shows how to display common information for an access point:

```
Device# show ap name AP01 config general

Cisco AP Name                                   : AP01
Cisco AP Identifier                             : 5
Country Code                                    : US  - United States
Regulatory Domain Allowed by Country            : 802.11bg:-A     802.11a:-A
AP Country Code                                 : US  - United States
AP Regulatory Domain                            : Unconfigured
Switch Port Number                              : 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
```

```
Tertiary Cisco Controller Name                    :
Tertiary Cisco Controller IP Address              : Not Configured
Administrative State                              : Enabled
Operation State                                   : Registered
AP Mode                                           : Local
AP Submode                                        : Not Configured
Remote AP Debug                                   : Disabled
Logging Trap Severity Level                       : informational
Software Version                                  : 7.4.0.5
Boot Version                                      : 7.4.0.5
Stats Reporting Period                            : 180
LED State                                         : Enabled
PoE Pre-Standard Switch                           : Disabled
PoE Power Injector MAC Address                    : Disabled
Power Type/Mode                                   : Power Injector/Normal Mode
Number of Slots                                   : 2
AP Model                                          : 1140AG
AP Image                                          : C1140-K9W8-M
IOS Version                                       :
Reset Button                                      :
AP Serial Number                                  : SIM1140K001
AP Certificate Type                               : Manufacture Installed
Management Frame Protection Validation            : Disabled
AP User Mode                                      : Customized
AP User Name                                      : cisco
AP 802.1X User Mode                               : Not Configured
AP 802.1X User Name                               : Not Configured
Cisco AP System Logging Host                      : 255.255.255.255
AP Up Time                                        : 15 days 16 hours 19 minutes 57
 seconds
AP CAPWAP Up Time                                 : 4 minutes 56 seconds
Join Date and Time                                : 10/18/2012 04:48:56
Join Taken Time                                   : 15 days 16 hours 15 minutes 0
seconds
Join Priority                                     : 1
Ethernet Port Duplex                              : Auto
Ethernet Port Speed                               : Auto
AP Link Latency                                   : Disabled
Rogue Detection                                   : Disabled
AP TCP MSS Adjust                                 : Disabled
AP TCP MSS Size                                   : 6146
```

# show ap name config slot

To display the configuration of a Cisco AP and also display the common information for a slot, use the **show ap name config slot** command.

**show ap name** *Cisco-ap-name* **slot** *0-3*

## Syntax Description

| | |
|---|---|
| *Cisco-ap-name* | Specifies the name of the Cisco AP. |
| *0-3* | Specifies the slot ID. |

## Command Default

None

## Command Modes

Any command mode

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

### Example

This example shows how to display common information for a slot in an access point:

```
Device# show ap name Cisco-ap-name config slot 3
```

# show ap name config ethernet

To see Ethernet related configuration information of an AP, use the **show ap name** *ap-name* **config ethernet** command.

**show ap name** *ap-name* **config ethernet** [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

## Syntax Description

| | |
|---|---|
| *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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see Ethernet related configuration information of an AP:

```
Device# show ap name my-ap config ethernet
```

# show ap name dot11

To display 802.11a or 802.11b configuration information that corresponds to specific Cisco lightweight access points, use the **show ap name dot11** command.

**show ap name** *ap-name* **dot11** { **24ghz** | **5ghz** } { **ccx** | **cdp** | **profile** | **service-policy output** | **tsm** { **all** *client-mac* } }

## Syntax Description

| | |
|---|---|
| *ap-name* | Name of the Cisco lightweight access point. |
| **24ghz** | Displays the 2.4-GHz band. |
| **5ghz** | Displays the 5-GHz band. |
| **ccx** | Displays the Cisco Client eXtensions (CCX) radio management status information. |
| **cdp** | Displays Cisco Discovery Protocol (CDP) information. |
| **profile** | Displays configuration and statistics of 802.11 profiling. |
| **service-policy output** | Displays downstream service policy information. |
| **tsm** | Displays 802.11 traffic stream metrics statistics. |
| **all** | Displays the list of all access points to which the client has associations. |
| *client-mac* | MAC address of the client. |
| **SI** | Displays the SI configurations. |
| **airtime-fairness** | Displays the stats of 24Ghz or 5Ghz airtime-fairness. |
| **call-control** | Displays the call control information. |
| **radio-reset** | Displays radio-reset. |
| **slot** | Displays slot information. |
| **voice** | Displays voice information. |

## Command Default

None

## Command Modes

Any command mode

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to display the service policy that is associated with the access point:

```
Device# show ap name test-ap dot11 24ghz service-policy output

Policy Name  : test-ap1
Policy State : Installed
```

This example shows how to display the CCX RRM 802.11 configuration for a specific access point:

```
Device# show ap name AP01 dot11 24ghz ccx
```

This example show how to display CDP information for a specific access point:

```
Device# show ap name AP01 dot11 24ghz cdp

AP Name               AP CDP State
--------------------- --------------
AP03                  Disabled
```

This example show how to display the configuration and statistics of 802.11b profiling for a specific access point:

```
Device# show ap name AP01 dot11 24ghz profile

 802.11b Cisco AP performance profile mode             : GLOBAL
 802.11b Cisco AP Interference threshold               : 10 %
 802.11b Cisco AP noise threshold                      : -70 dBm
 802.11b Cisco AP RF utilization threshold             : 80 %
 802.11b Cisco AP throughput threshold                 : 1000000 bps
 802.11b Cisco AP clients threshold                    : 12 clients
```

This example show how to display downstream service policy information for a specific access point:

```
Device# show ap name AP01 dot11 24ghz service-policy output

Policy Name  : def-11gn
Policy State : Installed
```

This example show how to display the traffic stream configuration for all clients that correspond to a specific access point:

```
Device# show ap name AP01 dot11 24ghz tsm all
```

# show ap name 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see the AP environment information of an AP:

```
Device# show ap name my-ap environment
```

# show ap name gps location

To see the GPS location of the AP, use the **show ap name gps location** command.

**show ap name** *ap-name* **gps location** [ {*chassis-number* | **active** | **standby**}**R0**

## Syntax Description

| | |
|---|---|
| *ap-name* | Name of the Access Point |
| **gps** | See the GPS information of a Cisco AP |
| **location** | Shows the Mesh linktest data |
| *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 configuration in Route-processor slot 0. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see the GPS location of an AP:

```
Device# show ap name mesh-profile-name gps location
```

# show ap name hyperlocation

To view a summary or detailed information about the hyperlocation configuration for an access point (AP), use the **show ap name hyperlocation** command.

**show ap name** *ap-name* **hyperlocation ble-beacon**

## Syntax Description

| | |
|---|---|
| *ap-name* | Access point name. |
| **hyperlocation** | Displays AP hyperlocation information. |
| **ble-beacon** | Displays BLE beacon configuration of an AP. |

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Denali 16.3.1 | This command was introduced. |

### Example

This example shows how to view the BLE beacon configuration of an AP:

```
Device# show ap name test-ap hyperlocation ble-beacon

ID  Major  Minor  TX Power(dBm)
-------------------------------
0   0      0      0
1   0      0      0
2   0      0      0
3   0      0      0
```

# show ap name mesh backhaul

To see mesh backhaul statistics of an AP, use the **show ap name** *ap-name* **mesh backhaul** command.

**show ap name** *ap-name* **mesh backhaul** [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

## Syntax Description

| | |
|---|---|
| *chassis-number* | Enter the chassis number as either 1 or 2. |
| **active R0** | Active instance of the AP filters in Route-processor slot 0. |
| **standby R0** | Standby instance of the AP filters in Route-processor slot 0. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see mesh backhaul statistics of an AP:

```
Device# show ap name mymeshap mesh backhaul
```

# show ap name mesh bhrate

To see mesh 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**]

| | |
|---|---|
| *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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see mesh 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**]

## Syntax Description

| | |
|---|---|
| *ap-name* | Name of the Access Point |
| **linktest** | Shows the Mesh linktest |
| **data** | Shows the Mesh linktest data |
| *dest-mac* | Enter the AP MAC address. |
| *chassis-number* | Enter the chassis number as either 1 or 2. |
| **active R0** | Active instance of the configuration in Route-processor slot 0. |
| **standby R0** | Standby instance of the configuration in Route-processor slot 0. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see the mesh linktest data of an AP:

```
Device# show ap name mesh-profile-namemesh 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see detailed information about a neighbor of a mesh AP:

```
Device# show ap name mymeshap mesh neighbhor detail
```

# show ap name mesh neighbor detail

To see detailed information about a neighbor of a mesh AP, use the **show ap name** *ap-name* **mesh neighbor detail** command.

**show ap name** *ap-name* **mesh neighbor detail** [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

## Syntax Description

| | |
|---|---|
| *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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see detailed information about a neighbor of a mesh AP:

```
Device# show ap name mymeshap mesh neighbhor detail
```

# show ap name mesh path

To see information about the mesh AP's path, use the **show ap name** *ap-name* **mesh path** command.

**show ap name** *ap-name* **mesh path** [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

## Syntax Description

| | |
|---|---|
| *chassis-number* | Enter the chassis number as either 1 or 2. |
| **active R0** | Active instance of the AP filters in Route-processor slot 0. |
| **standby R0** | Standby instance of the AP filters in Route-processor slot 0. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see information about the mesh AP's path:

```
Device# show ap name mymeshap mesh path
```

# show ap name mesh stats

To see mesh statistics, use the **show ap name** *ap-name* **mesh stats** command.

**show ap name** *ap-name*[**packet error** | **queue** | **security**]

## Syntax Description

| | |
|---|---|
| *ap-name* | Name of the AP. |
| **packet error** | Mesh packet error statistics. |
| **queue** | Mesh queue statistics. |
| **security** | Mesh security statistics. |
| *chassis-number* | Enter the chassis number as either 1 or 2. |
| **active R0** | Active instance of the AP filters in Route-processor slot 0. |
| **standby R0** | Standby instance of the AP filters in Route-processor slot 0. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see mesh 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.

**show ap name** *ap-name* **wlan** {**dot11** {**24ghz** | **5ghz**} | **statistic**}

## Syntax Description

| | |
|---|---|
| *ap-name* | Name of the Cisco lightweight access point. |
| **dot11** | Displays 802.11 parameters. |
| **24ghz** | Displays 802.11b network settings. |
| **5ghz** | Displays 802.11a network settings. |
| **statistic** | Displays WLAN statistics. |

## Command Default

None

## Command Modes

Any command mode

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to display BSSID information of an access point in an 802.11b network:

```
Device# show ap name AP01 wlan dot11 24ghz

Site Name                                         : default-group
Site Description                                  :

WLAN ID  Interface  BSSID
-------------------------------------
1        default    00:00:20:00:02:00
12       default    00:00:20:00:02:0b
```

This example shows how to display WLAN statistics for an access point:

```
Device# show ap name AP01 wlan statistic

WLAN ID  : 1
WLAN Profile Name  : maria-open

   EAP Id Request Msg Timeouts           : 0
   EAP Id Request Msg Timeouts Failures  : 0
   EAP Request Msg Timeouts              : 0
   EAP Request Msg Timeouts Failures     : 0
   EAP Key Msg Timeouts                  : 0
   EAP Key Msg Timeouts Failures         : 0


WLAN ID  : 12
WLAN Profile Name  : 24
```

```
EAP Id Request Msg Timeouts           : 0
EAP Id Request Msg Timeouts Failures  : 0
EAP Request Msg Timeouts              : 0
EAP Request Msg Timeouts Failures     : 0
EAP Key Msg Timeouts                  : 0
EAP Key Msg Timeouts Failures         : 0
```

# show ap name temperature

To view the temperature information of an AP, use the **show ap name temperature** command.

**show ap name** *ap-name* **temperature**

### Syntax Description

| | |
|---|---|
| *ap-name* | AP name. |

### Command Default

None

### Command Modes

Privileged EXEC (#)

### Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Amsterdam 17.3.1 | This command was introduced. |

### Examples

This example shows how to view the temperature information of an AP:

```
Device# show ap name ap-3702 temperature
```

# show ap 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

| | |
|---|---|
| *profile-name* | AP profile name. |
| **detailed** | Shows the detailed parameters of the AP join profile. |
| **hyperlocation** | Shows Hyperlocation information for the AP profile. |
| **ble-beacon** | Show the list of configured BLE beacons for the AP profile. |
| **detail** | Shows detailed status of Hyperlocation for the AP profile. |
| **summary** | Shows overall status of Hyperlocation for the AP profile |
| *chassis-number* | Chassis number as either 1 or 2. |
| **active R0** | Active instance in Route-processor slot 0. |
| **standby R0** | Standby instance in Route-processor slot 0. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

## Examples

The following example shows how to see the overall status of Hyperlocation for an AP profile:

```
Device# show ap profile my-ap-profile detailed
```

# show ap rf-profile name

To display the selected ap RF-Profile details, use the **show ap rf-profile name** command.

**show ap rf-profile name** *profile-name* **detail**

## Syntax Description

| | |
|---|---|
| *profile-name* | Name of the RF-Profile. |
| **detail** | Show detail of selected RF Profile. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Denali 16.3.1 | This command was introduced. |

## Usage Guidelines

None

This example shows how to display the details of the selected RF-Profile.

```
Device#show ap rf-profile name doctest detail
Description :
AP Group Names :
RF Profile Name : doctest
Band : 2.4 GHz
802.11n client only : Disabled
Transmit Power Threshold v1: -70 dBm
Min Transmit Power: -10 dBm
Max Transmit Power: 30 dBm
Operational Rates
  802.11b 1M Rate : Mandatory
  802.11b 2M Rate : Mandatory
  802.11b 5.5M Rate : Mandatory
  802.11b 11M Rate : Mandatory
  802.11b 6M Rate : Mandatory
  802.11b 9M Rate : Supported
  802.11b 12M Rate : Supported
  802.11b 18M Rate : Supported
  802.11b 24M Rate : Supported
  802.11b 36M Rate : Supported
  802.11b 48M Rate : Supported
  802.11b 54M Rate : Supported
Max Clients : 200
Wlan name                       Max Clients
--------------------------------------------

Trap Threshold
  Clients:  12 clients
  Interference:  10%
  Noise:  -70 dBm
  Utilization:  80%
Multicast Data Rate: auto
Rx SOP Threshold : auto
Band Select
```

```
  Probe Response:  Disabled
  Cycle Count:  2 cycles
  Cycle Threshold:  200 milliseconds
  Expire Suppression:  20 seconds
  Expire Dual Band:  60 seconds
  Client RSSI:  -80 dBm
  Client Mid RSSI:  -80 dBm
Load Balancing
  Window:  5 clients
  Denial:  3 count
Coverage Data
  Data: -80 dBm
  Voice: -80 dBm
 Minimum Client Level: 3 clients
  Exception Level: 25%
DCA Channel List  : 1,5,9,13
DCA Foreign AP Contribution : Enabled
802.11n MCS Rates
  MCS 0 : Enabled
  MCS 1 : Enabled
  MCS 2 : Enabled
  MCS 3 : Enabled
  MCS 4 : Enabled
  MCS 5 : Enabled
  MCS 6 : Enabled
  MCS 7 : Enabled
  MCS 8 : Enabled
  MCS 9 : Enabled
  MCS 10 : Enabled
  MCS 11 : Enabled
  MCS 12 : Enabled
  MCS 13 : Enabled
  MCS 14 : Enabled
  MCS 15 : Enabled
  MCS 16 : Enabled
  MCS 17 : Enabled
  MCS 18 : Enabled
  MCS 19 : Enabled
  MCS 20 : Enabled
  MCS 21 : Enabled
  MCS 22 : Enabled
  MCS 23 : Enabled
  MCS 24 : Enabled
  MCS 25 : Enabled
  MCS 26 : Enabled
  MCS 27 : Enabled
  MCS 28 : Enabled
  MCS 29 : Enabled
  MCS 30 : Enabled
  MCS 31 : Enabled
State : Down
```

# show ap rf-profile summary

To display the ap RF-Profile summary, use the **show ap rf-profile summary** command.

**show ap rf-profile summary**

### Syntax Description

| | |
|---|---|
| **summary** | Show summary of RF Profiles |

### Command Default

None

### Command Modes

Privileged EXEC

### Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Denali 16.3.1 | This command was introduced. |

### Usage Guidelines

None

This example shows how to display the ap RF-Profile summary .

```
Device#show ap rf-profile summary
Number of RF Profiles : 1

RF Profile Name                  Band      Description          Applied   State
----------------------------------------------------------------------------------
doctest                          2.4 GHz                        No        Down
```

# show ap summary

To display the status summary of all Cisco lightweight access points attached to the device, use the **show ap summary** command.

**show ap summary**

### Syntax Description

| |
|---|
| This command has no keywords and arguments. |

### Command Default

None

### Command Modes

Any command mode

### Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

### Usage Guidelines

Use this command to display a list that contains each lightweight access point name, number of slots, manufacturer, MAC address, location, and the device port number.

This example shows how to display a summary of all connected access points:

```
Controller# show ap summary

Number of APs: 1

Global AP User Name: Cisco
Global AP Dot1x User Name: Not configured

AP Name                          AP Model  Ethernet MAC    Radio MAC       State
-------------------------------------------------------------------------------------
3602a                            3502I     003a.99eb.3fa8  d0c2.8267.8b00  Registered
```

# show ap tag sources

To see AP tag sources with priorities, use the **show ap tag sources** command.

**show ap tag sources** [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

## Syntax Description

| | |
|---|---|
| *chassis-number* | Chassis number as either 1 or 2. |
| **active R0** | Active instance of the AP filters in Route-processor slot 0. |
| **standby R0** | Standby instance of the AP filters in Route-processor slot 0. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see the AP tag sources with priorities for the active instance:

```
Device# show ap tag sources chassis active R0
```

# show ap tag summary

To view brief summary of tag names, use the **show ap tag summary** command.

**show ap tag summary**

| Syntax Description | |
|---|---|
| | This command has no keywords or arguments. |

**Command Default**

None

**Command Modes**

Privileged EXEC

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

### Example

The following example shows how to view brief summary of tag names:

```
Device# show ap tag summary
```

# show ap upgrade

To see AP upgrade information, use the **show ap upgrade** command.

**show ap upgrade** [**name** *ap-upgrade-report-name* | **summary** | **chassis** {*chassis-number* | **active** | **standby**}]

## Syntax Description

| | |
|---|---|
| **name** *ap-upgrade-report-name* | Enter the name of the AP upgrade report. |
| **summary** | Shows a summary of AP upgrade information. |
| *chassis-number* | Enter the chassis number as either 1 or 2. |
| **active R0** | Active instance in Route-processor slot 0. |
| **standby R0** | Standby instance in Route-processor slot 0. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see a summary of the AP upgrade information:

```
Device# show ap upgrade summary
```

# show ap upgrade method

To verify the status of the configuration of the image download over HTTPS method, use the **show ap upgrade method** command.

**show ap upgrade method**

## Syntax Description

This command has no keywords or arguments.

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Dublin 17.11.1 | This command was introduced. |

## Examples

The following example shows how to verify the status of HTTPS image download configuration:

```
Device# show ap upgrade method

AP upgrade method https : Enabled
```

# show arp

To view the ARP table, use the **show arp** command.

**show arp**

## Syntax Description

| | |
|---|---|
| **arp** | Shows ARP table |

## Command Modes

User EXEC (>)

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

The following example shows a sample output of the command:

```
Device# show arp

Address Age (min)      Hardware Addr
   9.11.8.1          0 84:80:2D:A0:D2:E6
9.11.32.111          0 3C:77:E6:02:33:3F
```

# show arp summary

To see the ARP table summary, use the **show arp summary** command.

**show arp summary**

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see the ARP table summary:

```
Device# show arp summary
```

# show ap upgrade site

To view the upgrade site-related infromation, use the **show ap upgrade site** command.

**show ap upgrade site** [ **summary** ]

## Syntax Description

| | |
|---|---|
| **summary** | (Optional) Displays a summary of access point (AP) upgrade on individual sites. |

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Cupertino 17.9.1 | This command was introduced. |

## Examples

The following example shows how to view the upgrade site-related infromation:

```
Device# show ap upgrade site

Site-filtered AP upgrade report data
====================================
Source controller: Controller1
Destination controller: Controller2
Site-filters present: Yes

AP image upgrade site summary
-----------------------------
Operation: N+1 move

Site Tag                                  Status
---------------------------------------------------------
site1                                     In Progress

AP upgrade reports linked to these site-filters
-----------------------------------------------

Start time               Operation type             Report name
------------------------------------------------------------------------
01/30/2022 10:34:36 IST  AP image upgrade/move CLI  AP_upgrade_to_Controller2_3002022103435
```

# show avc client

To display information about top number of applications, use the **show avc client** command in privileged EXEC mode.

**show avc client** *client-mac* **top** *n* **application** [**aggregate** | **upstream** | **downstream**]

## Syntax Description

| | |
|---|---|
| **client** *client-mac* | Specifies the client MAC address. |
| **top** *n* **application** | Specifies the number of top "N" applications for the given client. |

## Command Default

No default behavior or values.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

The following is sample output from the **show avc client** command:

```
Device# sh avc client 0040.96ae.65ec top 10 application aggregate

Cumulative Stats:

No.  AppName      Packet-Count    Byte-Count       AvgPkt-Size     usage%
---------------------------------------------------------------------------
1    skinny         7343            449860           61              94
2    unknown        99              13631            137             3
3    dhcp           18              8752             486             2
4    http           18              3264             181             1
5    tftp           9               534              59              0
6    dns            2               224              112             0

Last Interval(90 seconds) Stats:

No.  AppName     Packet-Count     Byte-Count       AvgPkt-Size      usage%
----------------------------------------------------------------------------
1    skinny         9               540              60               100
```

# show avc wlan

To display information about top applications and users using the applications, use the **show avc wlan** command in privileged EXEC mode.

**show avc wlan** *ssid* **top** *n* **application** [**aggregate** | **upstream** | **downstream**]

## Syntax Description

| | |
|---|---|
| **wlan** *ssid* | Specifies the Service Set IDentifier (SSID) for WLAN. |
| **top** *n* **application** | Specifies the number of top "N" applications. |

## Command Default

No default behavior or values.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

The following is sample output from the **show avc wlan** command:

```
Device# show avc wlan Lobby_WLAN top 10 application aggregate

Cumulative Stats:

No.  AppName           Packet-Count          Byte-Count          AvgPkt-Size  usage%
--------------------------------------------------------------------------------------
1    ssl                10598677              1979525706            997          42
2    vnc                5550900               3764612847            678          14
3    http               3043131               2691327197            884          10
4    unknown            1856297               1140264956            614          4
5    video-over-http    1625019               2063335150            1269         8
6    binary-over-http   1329115               1744190344            1312         6
7    webex-meeting      1146872               540713787             471          2
8    rtp                923900                635650544             688          2
9    unknown            752341                911000213             1210         3
10   youtube            631085                706636186             1119         3

Last Interval(90 seconds) Stats:

No.  AppName          Packet-Count          Byte-Count            AvgPkt-Size  usage%
---------------------------------------------------------------------------------------
1    vnc                687093                602731844             877          68
2    video-over-http    213272                279831588             1312         31
3    ssl                6515                  5029365               771          1
4    webex-meeting      3649                  1722663               472          0
5    http               2634                  1334355               506          0
6    unknown            1436                  99412                 69           0
7    google-services    722                   378121                523          0
8    linkedin           655                   393263                600          0
9    exchange           432                   167390                387          0
10   gtalk-chat         330                   17330                 52           0
```

# show chassis

To see the chassis information, use the **show chassis** command.

**show chassis** [*1 2* | **detail** | **mode** | **neighbors** | **ha-status** {**active** | **local** | **standby**}]

## Syntax Description

| | |
|---|---|
| {*1* \| *2*} | Chassis number as 1 or 2 to see the information about the relevant chassis. |
| **detail** | Shows detailed information about the chassis. |
| **mode** | Shows information about the chassis mode. |
| **neighbors** | Shows information about the chassis neighbors. |
| **ha-status** | Option to see information about the High Availability (HA) status. |
| **active** | Shows HA status on the chassis that is in active state. |
| **local** | Shows HA status on the local chassis. |
| **standby** | Shows HA status on the chassis that is in standby state. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see the HA status on the active chassis:

```
Device# show chassis ha-status active
```

# show checkpoint

To display information about the Checkpoint Facility (CF) subsystem, use the **show checkpoint** command.

**show checkpoint** { **clients** *client-ID <0-381>* | **entities***entity-ID <1-7>* | **statisticsbuffer-usage** }

## Syntax Description

| | |
|---|---|
| **clients** | Displays detailed information about checkpoint clients. |
| **entities** | Displays detailed information about checkpoint entities. |
| **statistics** | Displays detailed information about checkpoint statistics. |
| **buffer-usage** | Displays the checkpoint statistics of clients using large number of buffers. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to display all the CF clients.

```
   Client residing in process  : 8135
--------------------------------------------------------------------------------
Checkpoint client: WCM_MOBILITY
    Client ID                   : 24105
    Total DB inserts            : 0
    Total DB updates            : 0
    Total DB deletes            : 0
    Total DB reads              : 0
    Number of tables            : 6
    Client residing in process  : 8135
--------------------------------------------------------------------------------
Checkpoint client: WCM_DOT1X
    Client ID                   : 24106
    Total DB inserts            : 2
    Total DB updates            : 1312
    Total DB deletes            : 2
    Total DB reads              : 0
    Number of tables            : 1
    Client residing in process  : 8135
--------------------------------------------------------------------------------
Checkpoint client: WCM_APFROGUE
    Client ID                   : 24107
    Total DB inserts            : 0
    Total DB updates            : 0
    Total DB deletes            : 0
    Total DB reads              : 0
    Number of tables            : 1
    Client residing in process  : 8135
--------------------------------------------------------------------------------
Checkpoint client: WCM_CIDS
    Client ID                   : 24110
    Total DB inserts            : 0
    Total DB updates            : 0
    Total DB deletes            : 0
    Total DB reads              : 0
    Number of tables            : 0
    Client residing in process  : 8135
--------------------------------------------------------------------------------
Checkpoint client: WCM_NETFLOW
    Client ID                   : 24111
    Total DB inserts            : 7
    Total DB updates            : 0
    Total DB deletes            : 0
    Total DB reads              : 0
    Number of tables            : 1
    Client residing in process  : 8135
--------------------------------------------------------------------------------
Checkpoint client: WCM_MCAST
    Client ID                   : 24112
    Total DB inserts            : 0
    Total DB updates            : 0
    Total DB deletes            : 0
    Total DB reads              : 0
    Number of tables            : 1
    Client residing in process  : 8135
--------------------------------------------------------------------------------
Checkpoint client: wcm_comet
    Client ID                   : 24150
    Total DB inserts            : 0
    Total DB updates            : 0
    Total DB deletes            : 0
    Total DB reads              : 0
    Number of tables            : 0
    Client residing in process  : 8135
--------------------------------------------------------------------------------

All iosd checkpoint clients

--------------------------------------------------------------------------------
Client Name            Client     Entity     Bundle
                           ID         ID       Mode
--------------------------------------------------------------------------------
Network RF Client           3         --       Off

  Total API Messages Sent:                       0
  Total Transport Messages Sent:                 0
  Length of Sent Messages:                       0
  Total Blocked Messages Sent:                   0
  Length of Sent Blocked Messages:               0
  Total Non-blocked Messages Sent:               0
  Length of Sent Non-blocked Messages:           0
  Total Bytes Allocated:                         0
  Buffers Held:                                  0
  Buffers Held Peak:                             0
  Huge Buffers Requested:                        0
  Transport Frag Count:                          0
  Transport Frag Peak:                           0
  Transport Sends w/Flow Off:                    0
  Send Errs:                                     0
  Send Peer Errs:                                0
  Rcv Xform Errs:                                0
  Xmit Xform Errs:                               0
  Incompatible Messages:                         0
  Client Unbundles to Process Memory:            T
--------------------------------------------------------------------------------
Client Name            Client     Entity     Bundle
```

```
                           ID         ID       Mode
--------------------------------------------------------------------------------
SNMP CF Client             12         --       Off

  Total API Messages Sent:                       0
  Total Transport Messages Sent:                 0
  Length of Sent Messages:                       0
  Total Blocked Messages Sent:                   0
  Length of Sent Blocked Messages:               0
  Total Non-blocked Messages Sent:               0
  Length of Sent Non-blocked Messages:           0
  Total Bytes Allocated:                         0
  Buffers Held:                                  0
  Buffers Held Peak:                             0
  Huge Buffers Requested:                        0
  Transport Frag Count:                          0
  Transport Frag Peak:                           0
  Transport Sends w/Flow Off:                    0
  Send Errs:                                     0
  Send Peer Errs:                                0
  Rcv Xform Errs:                                0
  Xmit Xform Errs:                               0
  Incompatible Messages:                         0
  Client Unbundles to Process Memory:            T
--------------------------------------------------------------------------------
Client Name            Client     Entity     Bundle
                           ID         ID       Mode
--------------------------------------------------------------------------------
Online Diags HA            14         --       Off

  Total API Messages Sent:                       0
  Total Transport Messages Sent:                 0
  Length of Sent Messages:                       0
  Total Blocked Messages Sent:                   0
  Length of Sent Blocked Messages:               0
  Total Non-blocked Messages Sent:               0
  Length of Sent Non-blocked Messages:           0
  Total Bytes Allocated:                         0
  Buffers Held:                                  0
  Buffers Held Peak:                             0
  Huge Buffers Requested:                        0
  Transport Frag Count:                          0
  Transport Frag Peak:                           0
  Transport Sends w/Flow Off:                    0
  Send Errs:                                     0
  Send Peer Errs:                                0
  Rcv Xform Errs:                                0
  Xmit Xform Errs:                               0
  Incompatible Messages:                         0
  Client Unbundles to Process Memory:            T
--------------------------------------------------------------------------------
Client Name            Client     Entity     Bundle
                           ID         ID       Mode
--------------------------------------------------------------------------------
ARP                        22         --       Off

  Total API Messages Sent:                       0
  Total Transport Messages Sent:                 0
  Length of Sent Messages:                       0
  Total Blocked Messages Sent:                   0
  Length of Sent Blocked Messages:               0
  Total Non-blocked Messages Sent:               0
  Length of Sent Non-blocked Messages:           0
  Total Bytes Allocated:                         0
  Buffers Held:                                  0
  Buffers Held Peak:                             0
  Huge Buffers Requested:                        0
  Transport Frag Count:                          0
  Transport Frag Peak:                           0
  Transport Sends w/Flow Off:                    0
  Send Errs:                                     0
  Send Peer Errs:                                0
  Rcv Xform Errs:                                0
  Xmit Xform Errs:                               0
  Incompatible Messages:                         0
  Client Unbundles to Process Memory:            T
--------------------------------------------------------------------------------
Client Name            Client     Entity     Bundle
                           ID         ID       Mode
--------------------------------------------------------------------------------
Tableid CF                 27         --       Off

  Total API Messages Sent:                       0
  Total Transport Messages Sent:                 0
  Length of Sent Messages:                       0
  Total Blocked Messages Sent:                   0
  Length of Sent Blocked Messages:               0
  Total Non-blocked Messages Sent:               0
  Length of Sent Non-blocked Messages:           0
  Total Bytes Allocated:                         0
  Buffers Held:                                  0
  Buffers Held Peak:                             0
  Huge Buffers Requested:                        0
  Transport Frag Count:                          0
  Transport Frag Peak:                           0
  Transport Sends w/Flow Off:                    0
  Send Errs:                                     0
  Send Peer Errs:                                0
  Rcv Xform Errs:                                0
  Xmit Xform Errs:                               0
  Incompatible Messages:                         0
  Client Unbundles to Process Memory:            T
--------------------------------------------------------------------------------
Client Name            Client     Entity     Bundle
                           ID         ID       Mode
--------------------------------------------------------------------------------
Event Manager              33          0       Off

  Total API Messages Sent:                       0
  Total Transport Messages Sent:                --
  Length of Sent Messages:                       0
  Total Blocked Messages Sent:                   0
  Length of Sent Blocked Messages:               0
  Total Non-blocked Messages Sent:               0
  Length of Sent Non-blocked Messages:           0
  Total Bytes Allocated:                         0
  Buffers Held:                                  0
  Buffers Held Peak:                             0
  Huge Buffers Requested:                        0
  Transport Frag Count:                          0
  Transport Frag Peak:                           0
  Transport Sends w/Flow Off:                    0
  Send Errs:                                     0
  Send Peer Errs:                                0
  Rcv Xform Errs:                                0
  Xmit Xform Errs:                               0
  Incompatible Messages:                         0
  Client Unbundles to Process Memory:            T
```

```
--------------------------------------------------------------------------------
Client Name            Client     Entity     Bundle
                           ID         ID       Mode
--------------------------------------------------------------------------------
LAN-Switch Port Mana       35          0       Off

  Total API Messages Sent:                       0
  Total Transport Messages Sent:                --
  Length of Sent Messages:                       0
  Total Blocked Messages Sent:                   0
  Length of Sent Blocked Messages:               0
  Total Non-blocked Messages Sent:               0
  Length of Sent Non-blocked Messages:           0
  Total Bytes Allocated:                         0
  Buffers Held:                                  0
  Buffers Held Peak:                             0
  Huge Buffers Requested:                        0
  Transport Frag Count:                          0
  Transport Frag Peak:                           0
  Transport Sends w/Flow Off:                    0
  Send Errs:                                     0
  Send Peer Errs:                                0
  Rcv Xform Errs:                                0
  Xmit Xform Errs:                               0
  Incompatible Messages:                         0
  Client Unbundles to Process Memory:            T
--------------------------------------------------------------------------------
Client Name            Client     Entity     Bundle
                           ID         ID       Mode
--------------------------------------------------------------------------------
LAN-Switch PAgP/LACP       36          0       Off

  Total API Messages Sent:                       0
  Total Transport Messages Sent:                --
  Length of Sent Messages:                       0
  Total Blocked Messages Sent:                   0
  Length of Sent Blocked Messages:               0
  Total Non-blocked Messages Sent:               0
  Length of Sent Non-blocked Messages:           0
  Total Bytes Allocated:                         0
  Buffers Held:                                  0
  Buffers Held Peak:                             0
  Huge Buffers Requested:                        0
  Transport Frag Count:                          0
  Transport Frag Peak:                           0
  Transport Sends w/Flow Off:                    0
  Send Errs:                                     0
  Send Peer Errs:                                0
  Rcv Xform Errs:                                0
  Xmit Xform Errs:                               0
  Incompatible Messages:                         0
  Client Unbundles to Process Memory:            T
--------------------------------------------------------------------------------
Client Name            Client     Entity     Bundle
                           ID         ID       Mode
--------------------------------------------------------------------------------
LAN-Switch VLANs           39          0       Off

  Total API Messages Sent:                       0
  Total Transport Messages Sent:                --
  Length of Sent Messages:                       0
  Total Blocked Messages Sent:                   0
  Length of Sent Blocked Messages:               0
  Total Non-blocked Messages Sent:               0
  Length of Sent Non-blocked Messages:           0
  Total Bytes Allocated:                         0
  Buffers Held:                                  0
  Buffers Held Peak:                             0
  Huge Buffers Requested:                        0
  Transport Frag Count:                          0
  Transport Frag Peak:                           0
  Transport Sends w/Flow Off:                    0
  Send Errs:                                     0
  Send Peer Errs:                                0
  Rcv Xform Errs:                                0
```

This example shows how to display all the CF entities.

```
KATANA_DOC#show checkpoint entities
                         Check Point List of Entities

 CHKPT on ACTIVE server.

--------------------------------------------------------------------------------
Entity ID         Entity Name
--------------------------------------------------------------------------------
        0         CHKPT_DEFAULT_ENTITY

  Total API Messages Sent:             0
  Total Messages Sent:                 0
  Total Sent Message Len:              0
  Total Bytes Allocated:               0
  Total Number of Members:            10

  Member(s) of entity 0 are:
    Client ID          Client Name
------------------------------------------
          168          DHCP Snooping
          167          IGMP Snooping
           41          Spanning-tree
           40          AUTH MGR CHKPT CLIEN
           39          LAN-Switch VLANs
           33          Event Manager
           35          LAN-Switch Port Mana
           36          LAN-Switch PAgP/LACP
          158          Inline Power Checkpoint
```

This example shows how to display the CF statistics.

```
KATANA_DOC#show checkpoint statistics
        IOSd Check Point Status
 CHKPT on ACTIVE server.

Number Of Msgs In Hold Q:              0
CHKPT MAX Message Size:                0
TP MAX Message Size:               65503
CHKPT Pending Msg Timer:             100 ms

  FLOW_ON  total:                      0
  FLOW_OFF total:                      0
  Current FLOW status is:             ON
  Total API Messages Sent:             0
  Total Messages Sent:                 0
  Total Sent Message Len:              0
  Total Bytes Allocated:               0
  Rcv  Msg Q Peak:                     0
  Hold Msg Q Peak:                     0
```

```
Buffers Held Peak:                 0
Current Buffers Held:              0
Huge Buffers Requested:            0
```

# show cts environment data

To display the TrustSec environment data on the AP, use the **show cts environment data** command:

**show cts environment data**

## Syntax Description

This command has no arguments or keywords.

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco Amsterdam 17.1.1 | This command was introduced. |

## Examples

The following example shows the TrustSec environment data on the AP:

```
Device# show cts environment

CTS Environment Data
====================
Current state = COMPLETE
Last status   = Successful
Local Device SGT:
SGT tag = 0-07:Unknown
Server List Info:
Installed list: CTSServerList1-0001, 1 server(s):
Server: 8.109.0.85, port 1812, A-ID 9818EE1ECA02B7BFE359C28B30EA7E2A
Status = ALIVE
auto-test = FALSE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs
Security Group Name Table:
0-07:Unknown
2-00:TrustSec_Devices
3-00:Network_Services
4-00:Employees
5-00:Contractors
6-00:Guests
7-00:Production_Users
8-00:Developers
9-00:Auditors
10-00:Point_of_Sale_Systems
11-02:Production_Servers
12-00:Development_Servers
13-00:Test_Servers
14-00:PCI_Servers
15-00:BYOD
16-06:BGL15
17-00:BGL12
255-00:Quarantined_Systems
Environment Data Lifetime = 86400 secs
Last update time = 11:50:49 UTC Sun Jan 9 2022
Env-data expires in   0:00:28:54 (dd:hr:mm:sec)
Env-data refreshes in 0:00:28:54 (dd:hr:mm:sec)
```

```
Cache data applied = NONE
State Machine is running
```

# show cts role-based sgt-map all

To display the bindings of IP address and SGT source names on the AP, use the **show cts role-based sgt-map all** command:

**show cts role-based sgt-map all**

## Syntax Description

This command has no arguments or keywords.

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco Amsterdam 17.1.1 | This command was introduced. |

## Examples

The following example shows the bindings of IP address and SGT source names on the AP:

```
Device# show cts role-based stg-map all

Active IPv4-SGT Bindings Information
IP Address                                 SGT       Source
==========================================================================
8.73.1.101                                  16      LOCAL
8.73.1.102                                  16      LOCAL
8.73.1.103                                  16      LOCAL
8.73.1.104                                  16      LOCAL
8.73.1.105                                  16      LOCAL
8.73.1.106                                  16      LOCAL
8.73.1.107                                  16      LOCAL
8.73.1.108                                  16      LOCAL
8.73.1.109                                  16      LOCAL
8.73.1.110                                  16      LOCAL
8.73.1.111                                  16      LOCAL
8.73.1.112                                  16      LOCAL
8.73.1.113                                  16      LOCAL
8.73.1.114                                  16      LOCAL
8.73.1.115                                  16      LOCAL
8.73.1.116                                  16      LOCAL
8.73.1.117                                  16      LOCAL
8.73.1.118                                  16      LOCAL
8.73.1.119                                  16      LOCAL
8.73.1.120                                  16      LOCAL
8.73.1.121                                  16      LOCAL
8.73.1.122                                  16      LOCAL
8.73.1.123                                  16      LOCAL
8.73.1.124                                  16      LOCAL
8.73.1.125                                  16      LOCAL
8.73.1.126                                  16      LOCAL
8.73.1.127                                  16      LOCAL
8.73.1.128                                  16      LOCAL
8.73.1.129                                  16      LOCAL
8.73.1.130                                  16      LOCAL
8.73.1.131                                  16      LOCAL
```

```
8.73.1.132                                16      LOCAL
8.73.1.133                                16      LOCAL
8.73.1.134                                16      LOCAL
8.73.1.135                                16      LOCAL
8.73.1.136                                16      LOCAL
8.73.1.137                                16      LOCAL
8.73.1.138                                16      LOCAL
8.73.1.139                                16      LOCAL
8.73.1.140                                16      LOCAL
8.73.1.141                                16      LOCAL
8.73.1.142                                16      LOCAL
FD09:8::                                  16      LOCAL
FD09:8:73:0:4051:EB27:B4A2:F6DB           16      LOCAL
FD09:8:73:0:4C3C:1D75:81E0:DB94           16      LOCAL
FD09:8:73:0:5136:9045:9D11:E191           16      LOCAL
FD09:8:73:0:6903:B84E:5BDF:9D54           16      LOCAL
FD09:8:73:0:A9F8:7825:B07:75A8            16      LOCAL
FD09:8:73:0:B505:626B:51D7:6DB6           16      LOCAL
FD09:8:73:0:D0B4:3316:7CE9:8AE8           16      LOCAL
FD09:8:73:0:ECA8:F5E:CCF5:FFD7            16      LOCAL

IP-SGT Active Bindings Summary
============================================
Total number of LOCAL    bindings = 9
Total number of active   bindings = 9
```

# show cts role-based counters

To clear all role-based counters on the AP, use the **show cts role-based counters** command:

**show cts role-based counters**

## Syntax Description

This command has no arguments or keywords.

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco Amsterdam 17.1.1 | This command was introduced. |

## Examples

The following example shows the clear all role-based counters on the AP:

```
Device# show cts role-based counters

From  To   SW-Denied HW-Denied SW-Permitt HW-Permitt  SW-Monitor HW-Monitor
==========================================================================
*     *     0          0          0          178837189  0           0
16    0     0          0          0          39250482   0           0
16    16    0          52835      0          0          0           0
17    16    0          0          0          0          0           0
```

# show etherchannel summary

To show details on the ports, port-channel, and protocols in the controller, use the **show etherchannel summary** command.

**show ethernet summary**

This command has no arguments or keywords.

## Command Default

None

## Command Modes

Privileged Mode.

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows the details on the ports, port-channel, and protocols in the controller.

```
controller#show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
2      Po2(SD)         -
23     Po23(SD)        -
```

# show flow exporter

To display flow exporter status and statistics, use the **show flow exporter** command in privileged EXEC mode.

**show flow exporter** [**export-ids netflow-v9** | [**name**] *exporter-name* [**statistics** | **templates**] | **statistics** | **templates**]

## Syntax Description

| | |
|---|---|
| **export-ids netflow-v9** | (Optional) Displays the NetFlow Version 9 export fields that can be exported and their IDs. |
| **name** | (Optional) Specifies the name of a flow exporter. |
| *exporter-name* | (Optional) Name of a flow exporter that was previously configured. |
| **statistics** | (Optional) Displays statistics for all flow exporters or for the specified flow exporter. |
| **templates** | (Optional) Displays template information for all flow exporters or for the specified flow exporter. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

The following example displays the status and statistics for all of the flow exporters configured on a device:

```
Device# show flow exporter
Flow Exporter FLOW-EXPORTER-1:
  Description:              Exports to the datacenter
  Export protocol:          NetFlow Version 9
  Transport Configuration:
    Destination IP address: 192.168.0.1
    Source IP address:      192.168.0.2
    Transport Protocol:     UDP
    Destination Port:       9995
    Source Port:            55864
    DSCP:                   0x0
    TTL:                    255
    Output Features:        Used
```

This table describes the significant fields shown in the display:

*Table 9: show flow exporter Field Descriptions*

| Field | Description |
|---|---|
| Flow Exporter | The name of the flow exporter that you configured. |

| Field | Description |
|---|---|
| Description | The description that you configured for the exporter, or the default description User defined. |
| Transport Configuration | The transport configuration fields for this exporter. |
| Destination IP address | The IP address of the destination host. |
| Source IP address | The source IP address used by the exported packets. |
| Transport Protocol | The transport layer protocol used by the exported packets. |
| Destination Port | The destination UDP port to which the exported packets are sent. |
| Source Port | The source UDP port from which the exported packets are sent. |
| DSCP | The differentiated services code point (DSCP) value. |
| TTL | The time-to-live value. |
| Output Features | Specifies whether the **output-features** command, which causes the output features to be run on Flexible NetFlow export packets, has been used or not. |

The following example displays the status and statistics for all of the flow exporters configured on a device:

```
Device# show flow exporter name FLOW-EXPORTER-1 statistics
Flow Exporter FLOW-EXPORTER-1:
  Packet send statistics (last cleared 2w6d ago):
    Successfully sent:         0                     (0 bytes)
```

# show flow interface

To display the  configuration and status for an interface, use the **show flow interface** command in privileged EXEC mode.

**show flow interface** [*type number*]

## Syntax Description

| | |
|---|---|
| *type* | (Optional) The type of interface on which you want to display  accounting configuration information. |
| *number* | (Optional) The number of the interface on which you want to display  accounting configuration information. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Examples

The following example displays the  accounting configuration on Ethernet interfaces 0/0 and 0/1:

```
Device# show flow interface gigabitethernet1/0/1

Interface Ethernet1/0
        monitor:         FLOW-MONITOR-1
        direction:       Output
        traffic(ip):     on
Device# show flow interface gigabitethernet1/0/2
Interface Ethernet0/0
        monitor:         FLOW-MONITOR-1
        direction:       Input
        traffic(ip):     sampler SAMPLER-2#
```

The table below describes the significant fields shown in the display.

*Table 10: show flow interface Field Descriptions*

| Field | Description |
|---|---|
| Interface | The interface to which the information applies. |
| monitor | The name of the flow monitor that is configured on the interface. |
| direction: | The direction of traffic that is being monitored by the flow monitor.<br>The possible values are:<br>• Input—Traffic is being received by the interface.<br>• Output—Traffic is being transmitted by the interface. |

| Field | Description |
|---|---|
| traffic(ip) | Indicates if the flow monitor is in normal mode or sampler mode.<br>The possible values are:<br>• on—The flow monitor is in normal mode.<br>• sampler—The flow monitor is in sampler mode (the name of the sampler will be included in the display). |

# show flow monitor

To display the status and statistics for a  flow monitor, use the **show flow monitor** command in privileged EXEC mode.

## Syntax Description

| | |
|---|---|
| **name** | (Optional) Specifies the name of a flow monitor. |
| *monitor-name* | (Optional) Name of a flow monitor that was previously configured. |
| **cache** | (Optional) Displays the contents of the cache for the flow monitor. |
| **format** | (Optional) Specifies the use of one of the format options for formatting the display output. |
| **csv** | (Optional) Displays the flow monitor cache contents in comma-separated variables (CSV) format. |
| **record** | (Optional) Displays the flow monitor cache contents in record format. |
| **table** | (Optional) Displays the flow monitor cache contents in table format. |
| **statistics** | (Optional) Displays the statistics for the flow monitor. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

The **cache** keyword uses the record format by default.

The uppercase field names in the display output of the **show flowmonitor** *monitor-name* **cache** command are key fields that  uses to differentiate flows. The lowercase field names in the display output of the **show flow monitor** *monitor-name* **cache** command are nonkey fields from which  collects values as additional data for the cache.

## Examples

The following example displays the status for a flow monitor:

```
Device# show flow monitor FLOW-MONITOR-1

Flow Monitor FLOW-MONITOR-1:
  Description:       Used for basic traffic analysis
  Flow Record:       flow-record-1
  Flow Exporter:     flow-exporter-1
                     flow-exporter-2
  Cache:
    Type:              normal
    Status:            allocated
    Size:              4096 entries / 311316 bytes
    Inactive Timeout:  15 secs
    Active Timeout:    1800 secs
```

This table describes the significant fields shown in the display.

*Table 11: show flow monitor monitor-name Field Descriptions*

| Field | Description |
|---|---|
| Flow Monitor | Name of the flow monitor that you configured. |
| Description | Description that you configured or the monitor, or the default description User defined. |
| Flow Record | Flow record assigned to the flow monitor. |
| Flow Exporter | Exporters that are assigned to the flow monitor. |
| Cache | Information about the cache for the flow monitor. |
| Type | Flow monitor cache type. The value is always normal, as it is the only supported cache type. |
| Status | Status of the flow monitor cache.<br>The possible values are:<br>• allocated—The cache is allocated.<br>• being deleted—The cache is being deleted.<br>• not allocated—The cache is not allocated. |
| Size | Current cache size. |
| Inactive Timeout | Current value for the inactive timeout in seconds. |
| Active Timeout | Current value for the active timeout in seconds. |

The following example displays the status, statistics, and data for the flow monitor named FLOW-MONITOR-1:

This table describes the significant fields shown in the display.

The following example displays the status, statistics, and data for the flow monitor named FLOW-MONITOR-1 in a table format:

The following example displays the status, statistics, and data for the flow monitor named FLOW-MONITOR-IPv6 (the cache contains IPv6 data) in record format:

The following example displays the status and statistics for a flow monitor:

# show flow record

To display the status and statistics for a  flow record, use the **show flow record** command in privileged EXEC mode.

**show flow record** [[**name**] *record-name*]

## Syntax Description

| | |
|---|---|
| **name** | (Optional) Specifies the name of a flow record. |
| *record-name* | (Optional) Name of a user-defined flow record that was previously configured. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

The following example displays the status and statistics for FLOW-RECORD-1:

```
Device# show flow record FLOW-RECORD-1
flow record FLOW-RECORD-1:
  Description:        User defined
  No. of users:       0
  Total field space:  24 bytes
  Fields:
    match ipv6 destination address
    match transport source-port
    collect interface input
```

# show interfaces

To display the administrative and operational status of all interfaces or for a specified interface, use the **show interfaces** command in privileged EXEC mode.

**show interfaces** [*interface-id* | **vlan** *vlan-id*] [**accounting** | **capabilities** [**module** *number*] | **debounce** | **description** | **etherchannel** | **flowcontrol** | **private-vlan mapping** | **pruning** | **stats** | **status** [**err-disabled**] | **trunk**]

## Syntax Description

| | |
|---|---|
| *interface-id* | (Optional) ID of the interface. Valid interfaces include physical ports (including type, stack member , module, and port number) and port channels. The port channel range is 1 to 48. |
| **vlan** *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.<br>**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.<br>This option is not available if you entered a specific interface ID. |
| **description** | (Optional) Displays the administrative status and description set for an interface. |
| **etherchannel** | (Optional) Displays interface EtherChannel information. |
| **flowcontrol** | (Optional) Displays interface flow control information. |
| **private-vlan mapping** | (Optional) Displays private-VLAN mapping information for the VLAN switch virtual interfaces (SVIs). This keyword is not available if the switch is running the LAN base feature set. |
| **pruning** | (Optional) Displays trunk VTP pruning information for the interface. |
| **stats** | (Optional) Displays the input and output packets by switching the path for the interface. |
| **status** | (Optional) Displays the status of the interface. A status of unsupported in the Type field means that a non-Cisco small form-factor pluggable (SFP) module is inserted in the module slot. |

| | |
|---|---|
| **err-disabled** | (Optional) Displays interfaces in an error-disabled state. |
| **trunk** | (Optional) Displays interface trunk information. If you do not specify an interface, only information for active trunking ports appears. |

**Note** Though visible in the command-line help strings, the **crb**, **fair-queue**, **irb**, **mac-accounting**, **precedence**, **random-detect**, **rate-limit**, and **shape** keywords are not supported.

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

The **show interfaces capabilities** command with different keywords has these results:

- Use the **show interface capabilities module** *number* command to display the capabilities of all interfaces on that chassis in the stack. If there is no chassis with that module number in the stack, there is no output.
- Use the **show interfaces** *interface-id* **capabilities** to display the capabilities of the specified interface.
- Use the **show interfaces capabilities** (with no module number or interface ID) to display the capabilities of all interfaces in the stack.

This is an example of output from the **show interfaces** command for an interface on stack member 3:

```
Device# show interfaces gigabitethernet3/0/2
GigabitEthernet3/0/2 is down, line protocol is down (notconnect)
  Hardware is Gigabit Ethernet, address is 2037.064d.4381 (bia 2037.064d.4381)
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, Auto-speed, media type is 10/100/1000BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
```

This is an example of output from the **show interfaces** *interface* **description** command when the interface has been described as *Connects to Marketing* by using the **description** interface configuration command:

```
Device# show interfaces gigabitethernet1/0/2 description
Interface                      Status         Protocol Description
Gi1/0/2                        up             down     Connects to Marketing
```

This is an example of output from the **show interfaces** *interface-id* **pruning** command when pruning is enabled in the VTP domain:

```
Device# show interfaces gigabitethernet1/0/2 pruning
Port      Vlans pruned for lack of request by neighbor
Gi1/0/2   3,4

Port      Vlans traffic requested of neighbor
Gi1/0/2   1-3
```

This is an example of output from the **show interfaces stats** command for a specified VLAN interface:

```
Device# show interfaces vlan 1 stats
Switching path    Pkts In    Chars In    Pkts Out    Chars Out
     Processor    1165354   136205310      570800     91731594
   Route cache          0           0           0            0
         Total    1165354   136205310      570800     91731594
```

These are examples of output from the **show interfaces status** command for a specific interface when private VLANs are configured. Port 22 is configured as a private-VLAN host port. It is associated with primary VLAN 20 and secondary VLAN 25:

```
Device# show interfaces gigabitethernet1/0/22 status
Port       Name      Status     Vlan      Duplex      Speed      Type
Gi1/0/22             connected  20,25     a-full      a-100      10/100BaseTX
```

In this example, port 20 is configured as a private-VLAN promiscuous port. The display shows only the primary VLAN 20:

```
Device# show interfaces gigabitethernet1/0/20 status
Port       Name      Status     Vlan      Duplex      Speed      Type
Gi1/0/20             connected  20        a-full      a-100      10/100BaseTX
```

This is an example of output from the **show interfaces status err-disabled** command. It displays the status of interfaces in the error-disabled state:

```
Device# show interfaces status err-disabled
Port      Name       Status         Reason
Gi1/0/2              err-disabled   gbic-invalid
Gi2/0/3              err-disabled   dtp-flap
```

This is an example of output from the **show interfaces** *interface-id* **pruning** command:

```
Device# show interfaces gigabitethernet1/0/2 pruning
Port Vlans pruned for lack of request by neighbor


Device# show interfaces gigabitethernet1/0/1 trunk
Port        Mode             Encapsulation  Status        Native vlan
Gi1/0/1     on               802.1q         other         10

Port        Vlans allowed on trunk
Gi1/0/1     none

Port        Vlans allowed and active in management domain
Gi1/0/1     none

Port        Vlans in spanning tree forwarding state and not pruned
Gi1/0/1     none
```

# show inventory

To display the product inventory listing of all Cisco products installed in the networking device, use the **show inventory** command.

**show inventory** [ *entity-name* | [ **fru** | **oid** | **raw** ] *entity-name* ]

## Syntax Description

| | |
|---|---|
| *entity-name* | (Optional) Name of a Cisco entity (for example, chassis, backplane, module, or slot). A quoted string may be used to display very specific UDI information; for example "sfslot 1" shows the UDI information for slot 1 of an entity named sfslot. |
| **fru** | (Optional) To display the component details of the **fru** entities within the container hierarchy in Cisco products. |
| **oid** | (Optional) To display the vendor specific hardware registration number for each part of the device. |
| **raw** | (Optional) To view the information about all Cisco products—referred to as entities—installed in the Cisco networking device, even if the entities do not have a product ID (PID) value, a unique device identifier (UDI), or other physical identification. |

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

## Usage Guidelines

The **show inventory** command retrieves and displays inventory information about each Cisco product in the form of a UDI. The UDI is a combination of three separate data elements: a product identifier (PID), a version identifier (VID), and the serial number (SN).

The PID is the name by which the product can be ordered; it has been historically called the "Product Name" or "Part Number." This is the identifier that one would use to order an exact replacement part.

The VID is the version of the product. Whenever a product has been revised, the VID will be incremented. The VID is incremented according to a rigorous process derived from Telcordia GR-209-CORE, an industry guideline that governs product change notices.

The SN is the vendor-unique serialization of the product. Each manufactured product will carry a unique serial number assigned at the factory, which cannot be changed in the field. This is the means by which to identify an individual, specific instance of a product.

The UDI refers to each product as an entity. Some entities, such as a chassis, will have subentities like slots. Each entity will display on a separate line in a logically ordered presentation that is arranged hierarchically by Cisco entities.

Use the **show inventory** command without options to display a list of Cisco entities installed in the networking device that are assigned a PID.

## Examples

This example shows how to display the product inventory listing of a Cisco product installed in the networking device:

```
Device# show inventory

NAME: "module R0", DESCR: "Cisco C9800-CL Route Processor"
PID: C9800-CL-K9       , VID: V00  , SN: Jxx1xxxxx1x
```

# show ip

To view the IP information, use the **show ip** command.

## Syntax Description

| | |
|---|---|
| **access-lists** | Lists the IP access lists |
| **interface** | Displays the IP interface status and configuration |
| **brief** | Displays the brief summary of IP status and configuration |
| **route** | Displays the IP routing table |
| **tunnel** | Displays the IP tunnel information |
| **eogre** | Displays the EoGRE tunnel information |
| **domain** | Displays the EoGRE tunnel domain information |
| **forwarding-table** | Displays the EoGRE tunnel encapsulation and decapsulation information |
| **gateway** | Displays the EoGRE tunnel gateway information |
| **fabric** | Displays the IP fabric tunnel information |
| **summary** | Displays the information for all tunnels |

## Command Modes

User EXEC (>)

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 8.1.111.0 | This command was introduced. |

The following example shows how to view information about the lists the IP access lists:

```
cisco-wave2-ap# show ip access-lists
```

# show ip igmp snooping igmpv2-tracking

To display group and IP address entries, use the **show ip igmp snooping igmpv2-tracking** command in privileged EXEC mode.

**Note** The command displays group and IP address entries only for wireless multicast IGMP joins and not for wired joins. This command also displays output only if wireless multicast is enabled.

**show ip igmp snooping igmpv2-tracking**

## Syntax Description

This command has no arguments or keywords.

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

# show ip igmp snooping querier

To display the configuration and operation information for the IGMP querier that is configured on a device, use the **show ip igmp snooping querier**command in user EXEC mode.

**show ip igmp snooping querier** [**vlan** *vlan-id*] [**detail** ]

## Syntax Description

| | |
|---|---|
| **vlan** *vlan-id* | (Optional) Specifies a VLAN; Ranges are from 1—1001 and 1006—4094. |
| **detail** | (Optional) Displays detailed IGMP querier information. |

## Command Modes

User EXEC

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

Use the **show ip igmp snooping querier** command to display the IGMP version and the IP address of a detected device, also called a querier, that sends IGMP query messages. A subnet can have multiple multicast routers but only one IGMP querier. In a subnet running IGMPv2, one of the multicast routers is elected as the querier. The querier can be a Layer 3 device.

The **show ip igmp snooping querier** command output also shows the VLAN and the interface on which the querier was detected. If the querier is the device, the output shows the Port field as Router. If the querier is a router, the output shows the port number on which the querier was detected in the Port field.

The **show ip igmp snooping querier detail** user EXEC command is similar to the **show ip igmp snooping querier** command. However, the **show ip igmp snooping querier** command displays only the device IP address most recently detected by the device querier.

The **show ip igmp snooping querier detail** command displays the device IP address most recently detected by the device querier and this additional information:

- The elected IGMP querier in the VLAN
- The configuration and operational information pertaining to the device querier (if any) that is configured in the VLAN

Expressions are case sensitive, for example, if you enter | **exclude output**, the lines that contain "output" do not appear, but the lines that contain "Output" appear.

### Examples

The following is a sample output from the **show ip igmp snooping querier** command:

```
Device> show ip igmp snooping querier
Vlan      IP Address     IGMP Version        Port
-------------------------------------------------------
1         172.20.50.11   v3                  Gi1/0/1
2         172.20.40.20   v2                  Router
```

The following is a sample output from the **show ip igmp snooping querier detail** command:

```
Device> show ip igmp snooping querier detail

Vlan      IP Address     IGMP Version   Port
-------------------------------------------------------------
1         10.0.0.10      v2             Fa8/0/1
Global IGMP device querier status

--------------------------------------------------------
admin state                    : Enabled
admin version                  : 2
source IP address              : 0.0.0.0
query-interval (sec)           : 60
max-response-time (sec)        : 10
querier-timeout (sec)          : 120
tcn query count                : 2
tcn query interval (sec)       : 10
Vlan 1:   IGMP device querier status
--------------------------------------------------------
elected querier is 10.0.0.10         on port Fa8/0/1
--------------------------------------------------------
admin state                    : Enabled
admin version                  : 2
source IP address              : 10.1.1.65
query-interval (sec)           : 60
max-response-time (sec)        : 10
querier-timeout (sec)          : 120
tcn query count                : 2
tcn query interval (sec)       : 10
operational state              : Non-Querier
operational version            : 2
tcn query pending count        : 0
```

# show ip igmp snooping wireless mcast-spi-count

To display the statistics of the number of multicast stateful packet inspections (SPIs) per multicast group ID (MGID) sent to the device, use the **show ip igmp snooping wireless mcast-spi-count** command in privileged EXEC mode.

**show ip igmp snooping wireless mcast-spi-count**

This command has no arguments or keywords.

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

None

### Examples

This is an example of output from the **show ip igmp snooping wireless mcast-spi-count** command:

```
Device# show ip igmp snooping wireless mcast-spi-count

Stats for Mcast Client Add/Delete SPI Messages Sent to WCM

MGID    ADD MSGs        Del MSGs
---------------------------------
4160    1323            667
```

# show ip igmp snooping wireless mgid

To display multicast group ID (MGID) mappings, use the **show ip igmp snooping wireless mgid** command in privileged EXEC mode.

**show ip igmp snooping wireless mgid**

## Syntax Description

This command has no arguments or keywords.

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

None

### Examples

This is an example of output from the **show ip igmp snooping wireless mgid** command:

```
Device# show ip igmp snooping wireless mgid

Total number of L2-MGIDs    = 0

Total number of MCAST MGIDs = 0

 Wireless multicast is Enabled in the system
 Vlan     bcast   nonip-mcast   mcast    mgid    Stdby Flags
 1     Disabled   Disabled   Enabled    Disabled  0:0:1:0
 25    Disabled   Disabled   Enabled    Disabled  0:0:1:0
 34    Disabled   Disabled   Enabled    Disabled  0:0:1:0
 200   Disabled   Disabled   Enabled    Disabled  0:0:1:0
 1002  Enabled    Enabled    Enabled    Disabled  0:0:1:0
 1003  Enabled    Enabled    Enabled    Disabled  0:0:1:0
 1004  Enabled    Enabled    Enabled    Disabled  0:0:1:0
 1005  Enabled    Enabled    Enabled    Disabled  0:0:1:0

Index  MGID                  (S, G, V)
--------------------------------------------------------
```

# show ip nbar protocol-discovery wlan

To see NBAR protocol discovery statistics for a WLAN, use the **show ip nbar protocol-discovery wlan** command.

**show ip nbar protocol-discovery wlan** *wlan-name*

## Syntax Description

| | |
|---|---|
| *wlan-name* | Name of the WLAN. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see the NBAR protocol discovery statistics for a WLAN named *mywlan*:

```
Device# show ip nbar protocol-discovery wlan mywlan
```

# show ipv6 access-list

To display the contents of all current IPv6 access lists, use the **show ipv6 access-list** command in user EXEC or privileged EXEC mode.

**show ipv6 access-list** [*access-list-name*]

## Syntax Description

| | |
|---|---|
| *access-list-name* | (Optional) Name of access list. |

## Command Default

All IPv6 access lists are displayed.

## Command Modes

User EXEC

Privileged EXEC

## Command History

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

The **show ipv6 access-list** command provides output similar to the **show ip access-list** command, except that it is IPv6-specific.

## Examples

The following output from the **show ipv6 access-list** command shows IPv6 access lists named inbound, tcptraffic, and outbound:

```
Device# show ipv6 access-list
IPv6 access list inbound
    permit tcp any any eq bgp reflect tcptraffic (8 matches) sequence 10
    permit tcp any any eq telnet reflect tcptraffic (15 matches) sequence 20
    permit udp any any reflect udptraffic sequence 30
IPv6 access list tcptraffic (reflexive) (per-user)
    permit tcp host 2001:0DB8:1::1 eq bgp host 2001:0DB8:1::2 eq 11000 timeout 300 (time
       left 243) sequence 1
    permit tcp host 2001:0DB8:1::1 eq telnet host 2001:0DB8:1::2 eq 11001 timeout 300
    (time left 296) sequence 2
IPv6 access list outbound
    evaluate udptraffic
    evaluate tcptraffic
```

The following sample output shows IPv6 access list information for use with IPSec:

```
Device#  show ipv6 access-list
IPv6 access list Tunnel0-head-0-ACL (crypto)
     permit ipv6 any any (34 matches) sequence 1
IPv6 access list Ethernet2/0-ipsecv6-ACL (crypto)
     permit 89 FE80::/10 any (85 matches) sequence 1
```

The table below describes the significant fields shown in the display.

*Table 12: show ipv6 access-list Field Descriptions*

| Field | Description |
|---|---|
| ipv6 access list inbound | Name of the IPv6 access list, for example, inbound. |
| permit | Permits any packet that matches the specified protocol type. |
| tcp | Transmission Control Protocol. The higher-level (Layer 4) protocol type that the packet must match. |
| any | Equal to ::/0. |
| eq | An equal operand that compares the source or destination ports of TCP or UDP packets. |
| bgp | Border Gateway Protocol. The lower-level (Layer 3) protocol type that the packet must be equal to. |
| reflect | Indicates a reflexive IPv6 access list. |
| tcptraffic (8 matches) | The name of the reflexive IPv6 access list and the number of matches for the access list. The **clear ipv6 access-list** privileged EXEC command resets the IPv6 access list match counters. |
| sequence 10 | Sequence in which an incoming packet is compared to lines in an access list. Lines in an access list are ordered from first priority (lowest number, for example, 10) to last priority (highest number, for example, 80). |
| host 2001:0DB8:1::1 | The source IPv6 host address that the source address of the packet must match. |
| host 2001:0DB8:1::2 | The destination IPv6 host address that the destination address of the packet must match. |
| 11000 | The ephemeral source port number for the outgoing connection. |
| timeout 300 | The total interval of idle time (in seconds) after which the temporary IPv6 reflexive access list named tcptraffic will time out for the indicated session. |
| (time left 243) | The amount of idle time (in seconds) remaining before the temporary IPv6 reflexive access list named tcptraffic is deleted for the indicated session. Additional received traffic that matches the indicated session resets this value to 300 seconds. |
| evaluate udptraffic | Indicates the IPv6 reflexive access list named udptraffic is nested in the IPv6 access list named outbound. |

# show ipv6 mld snooping

Use the **show ipv6 mld snooping** command in EXEC mode to display IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping configuration of the switch or the VLAN.

**show ipv6 mld snooping** [**vlan** *vlan-id*]

## Syntax Description

| | |
|---|---|
| **vlan** *vlan-id* | (Optional) Specify a VLAN; the range is 1 to 1001 and 1006 to 4094. |

## Command Modes

User EXEC

Privileged EXEC

## Command History

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

Use this command to display MLD snooping configuration for the switch or for a specific VLAN.

VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in MLD snooping.

To configure the dual IPv4 and IPv6 template, enter the **sdm prefer dual-ipv4-and-ipv6** global configuration command and reload the switch.

## Examples

This is an example of output from the show ipv6 mld snooping vlan command. It shows snooping characteristics for a specific VLAN.

```
Device# show ipv6 mld snooping vlan 100
Global MLD Snooping configuration:
-------------------------------------------
MLD snooping : Enabled
MLDv2 snooping (minimal) : Enabled
Listener message suppression : Enabled
TCN solicit query : Disabled
TCN flood query count : 2
Robustness variable : 3
Last listener query count : 2
Last listener query interval : 1000
Vlan 100:
--------
MLD snooping : Disabled
MLDv1 immediate leave : Disabled
Explicit host tracking : Enabled
Multicast router learning mode : pim-dvmrp
Robustness variable : 3
Last listener query count : 2
Last listener query interval : 1000
```

This is an example of output from the **show ipv6 mld snooping** command. It displays snooping characteristics for all VLANs on the switch.

```
Device# show ipv6 mld snooping
Global MLD Snooping configuration:
-------------------------------------------
MLD snooping : Enabled
MLDv2 snooping (minimal) : Enabled
Listener message suppression : Enabled
TCN solicit query : Disabled
TCN flood query count : 2
Robustness variable : 3
Last listener query count : 2
Last listener query interval : 1000

Vlan 1:
--------
MLD snooping : Disabled
MLDv1 immediate leave : Disabled
Explicit host tracking : Enabled
Multicast router learning mode : pim-dvmrp
Robustness variable : 1
Last listener query count : 2
Last listener query interval : 1000

<output truncated>

Vlan 951:
--------
MLD snooping : Disabled
MLDv1 immediate leave : Disabled
Explicit host tracking : Enabled
Multicast router learning mode : pim-dvmrp
Robustness variable : 3
Last listener query count : 2
Last listener query interval : 1000
```

# show ipv6 mld snooping querier vlan

To see IPv6 MLD querier information in a VLAN, use the **show ipv6 mld snooping querier vlan** command.

**show ipv6 mld snooping querier vlan** *vlan-id*

## Syntax Description

| | |
|---|---|
| *vlan-id* | VLAN ID. Valid range is 1 to 1001 and 1006 to 4094. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see the IPv6 MLD querier information in a VLAN whose ID is 3:

```
Device# show ipv6 mld snooping querier vlan 3
```

# show ipv6 mld snooping wireless mgid

To see multicast group identifer (MGID) mapping information in the IPv6 MLD wireless related snooping events, use the **show ipv6 mld snooping wireless mgid** command.

**show ipv6 mld snooping wireless mgid**

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see multicast group identifer (MGID) mapping information in the IPv6 MLD wireless related snooping events:

```
Device# show ipv6 mld snooping wireless mgid
```

# show ldap attributes

To view information about the default LDAP attribute mapping, use the **show ldap attributes** command.

**show ldap attributes**

## Syntax Description

| |
|---|
| This command has no arguments. |

## Command Default

None

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view information about the default LDAP attribute mapping:

```
Device# show ldap attributes
LDAP Attribute                     Format     AAA Attribute
==============                     ======     =============
airespaceBwDataBurstContract       Ulong      bsn-data-bandwidth-burst-contr
userPassword                       String     password
airespaceBwRealBurstContract       Ulong      bsn-realtime-bandwidth-burst-c
employeeType                       String     employee-type
airespaceServiceType               Ulong      service-type
airespaceACLName                   String     bsn-acl-name
priv-lvl                           Ulong      priv-lvl
memberOf                           String DN  supplicant-group
cn                                 String     username
airespaceDSCP                      Ulong      bsn-dscp
policyTag                          String     tag-name
airespaceQOSLevel                  Ulong      bsn-qos-level
airespace8021PType                 Ulong      bsn-8021p-type
airespaceBwRealAveContract         Ulong      bsn-realtime-bandwidth-average
airespaceVlanInterfaceName         String     bsn-vlan-interface-name
airespaceVapId                     Ulong      bsn-wlan-id
airespaceBwDataAveContract         Ulong      bsn-data-bandwidth-average-con
sAMAccountName                     String     sam-account-name
meetingContactInfo                 String     contact-info
telephoneNumber                    String     telephone-number
Map: att_map_1
department                         String DN  element-req-qos
```

# show ldap server

To view the LDAP server information, use the **show ldap server** command.

**show ldap server** { *server-name* | **all** }

## Syntax Description

| | |
|---|---|
| *server-name* | Name of the server. |
| **all** | Information of all the servers. |

## Command Default

None

## Command Modes

Privileged EXEC(#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the LDAP server information:

```
Device# show ldap server all
```

# show license air entities

To display information about active APs, new APs, and deleted APs in connection with a Cisco Catalyst Wireless Controller, enter the **show license air entities** command in privileged EXEC mode.

**show license air entities** { **added** | **bulk** | **deleted** | **no-change** | **summary** }

## Syntax Description

| | |
|---|---|
| `added` | Displays the list of newly reported APs. A newly added AP is one that was not listed in the last RUM report that the product instance generated. |
| **bulk** | Displays the list of all currently active APs for the product instance |
| **deleted** | Displays the list of deleted APs. A delete AP is one that was listed as active APs in the last RUM report that the product instance generated but is now disconnected. |
| **no-change** | Displays the list of APs where there has been no change in the status since the last report. |
| **summary** | Displays the RUM report generation particulars and information about active APs, new APs, and deleted APs, and indicates by when an acknowledgement (ACK) must be installed on the product instance. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |
| Cisco IOS XE Amsterdam 17.3.2a | Command output was updated to display information relating to Smart Licensing Using Policy. |

## Usage Guidelines

**Smart Licensing**: If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing.

**Smart Licensing Using Policy**: If the software version on the device is Cisco IOS XE Amsterdam 17.3.2 or a later release, command output displays fields pertinent to Smart Licensing Using Policy.

## Examples

For information about fields shown in the display for the **show license air entities summary** command, see Table 13: show license air entities summary Field Descriptions, on page 839 .

For sample output, see

- #unique_650 unique_650_Connect_42_section_gtj_hjm_frb
- show license air entities summary on a Cisco Catalyst 9800-L Wireless Controller, on page 840

*Table 13: show license air entities summary Field Descriptions*

| Field | Description |
|---|---|
| Last license report time | When the last RUM report was generated, in the local time zone. |

| Field | Description |
|---|---|
| Upcoming license report time | When the next RUM report will be generated, in the local time zone. |
| No. of APs active at last report | Total number of APs listed as active APs in the last RUM report that was generated. |
| No. of APs newly added with last report | Number of new APs in the last RUM report that was generated.<br>For example, if the number displayed here is 2, this means the *last but one* RUM report did not list these 2 APs, and are therefore newly added in the last RUM report that the product instance generated. |
| No. of APs deleted with last report | Total number of APs deleted as of the last RUM report that was generated.<br>For example, if the number displayed here is 2, this means 2 APs were in the *last but one* RUM report, but were deleted in the *last* RUM report was generated. |

### show license air entities summary on a Cisco Catalyst 9800-L Wireless Controller

The following is sample output on a Cisco Catalyst 9800-L Wireless Controller. Note how the output on this device does not display the `License Ack expected within` field. Reporting requirements on all Cisco Catalyst Wireless Controllers (except Cisco Catalyst 9800-CL Wireless Controller) are as per the standard guidelines in the Smart Licensing Using Policy environment: Reporting is required if the policy (**show license status**) or system messages indicate that it is.

```
Device# show license air entities summary
Upcoming license report time...................: 15:13:27.403 IST Tue Oct 26 2021
No. of APs active at last report...............: 1
No. of APs newly added with last report.........: 1
No. of APs deleted with last report.............: 0
```

# show license all

To display all licensing information enter the **show license all** command in Privileged EXEC mode. This command displays status, authorization, UDI, and usage information, all combined.

**show license all**

## Syntax Description

This command has no keywords or arguments

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |
| Cisco IOS XE Amsterdam 17.3.2a | Command output was updated to display information relating to Smart Licensing Using Policy.<br>Command output no longer displays Smart Account and Virtual account information. |

## Usage Guidelines

**Smart Licensing**: If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing.

**Smart Licensing Using Policy**: If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2 or a later release, command output displays fields pertinent to Smart Licensing Using Policy.

This command concatenates the output of other **show license** commands, enabling you to display different kinds of licensing information together. For field descriptions, refer to the corresponding commands in the links provided below.

The `Smart Licensing Status` and `Account Information` sections of the **show license all** command corresponds with the output of the show license status, on page 854 command.

The `License Usage` section of the **show license all** command corresponds with the output of the show license usage, on page 872 command.

The `Product Information` section of the **show license all** command corresponds with the output of the show license udi, on page 871 command.

The `Agent Version` section of the **show license all** command displays the Smart Agent version and is available only in this command.

The `License Authorizations` section of the **show license all** command corresponds with the output of the show license authorization, on page 845 command.

The `Usage Report Summary` section of the **show license all** command corresponds with the output in the show license tech, on page 865 command.

### Examples

For sample output, see:

Example: show license all (Cisco Catalyst 9800-CL Wireless Controllers), on page 842

### Example: show license all (Cisco Catalyst 9800-CL Wireless Controllers)

The following is sample output of the **show license all** command on a Cisco Catalyst 9800-CL Wireless Controller. Similar output is displayed on all supported Cisco Catalyst Wireless Controllers.

```
Device# show license all

Smart Licensing Status
======================

Smart Licensing is ENABLED
License Reservation is ENABLED

Export Authorization Key:
  Features Authorized:
    <none>

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Transport Off

Miscellaneous:
  Custom Id: <empty>

Policy:
  Policy in use: Merged from multiple sources.
  Reporting ACK required: yes (CISCO default)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 365 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 90 (CISCO default)
    Reporting frequency (days): 90 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)

Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: <none>
  Reporting push interval: 0 (no reporting)
  Next ACK push check: Nov 01 20:31:46 2020 IST
  Next report push: <none>
  Last report push: <none>
  Last report file write: <none>

Trust Code Installed: <none>

License Usage
=============

air-network-advantage (DNA_NWStack):
  Description: air-network-advantage
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: air-network-advantage
  Feature Description: air-network-advantage
  Enforcement type: NOT ENFORCED
  License type: Perpetual
  Reservation:
    Reservation status: SPECIFIC INSTALLED
    Total reserved count: 20

air-dna-advantage (AIR-DNA-A):
  Description: air-dna-advantage
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: air-dna-advantage
  Feature Description: air-dna-advantage
  Enforcement type: NOT ENFORCED
  License type: Perpetual
  Reservation:
    Reservation status: SPECIFIC INSTALLED
    Total reserved count: 20

Product Information
===================
UDI: PID:C9800-CL-K9,SN:93BBAH93MGS

HA UDI List:
    Active:PID:C9800-CL-K9,SN:93BBAH93MGS
    Standby:PID:C9800-CL-K9,SN:9XECPSUU4XN

Agent Version
=============
Smart Agent for Licensing: 5.0.6_rel/47

License Authorizations
======================
Overall status:
  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
      Status: SPECIFIC INSTALLED on Nov 02 03:16:01 2020 IST
      Last Confirmation code: 102fc949
  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
      Status: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
      Last Confirmation code: ad4382fe

Specified license reservations:
  Aironet DNA Advantage Term Licenses (AIR-DNA-A):
    Description: DNA Advantage for Wireless
    Total reserved count: 20
    Enforcement type: NOT ENFORCED
    Term information:
      Active: PID:C9800-CL-K9,SN:93BBAH93MGS
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 5
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
          Start Date: 2020-JUN-18 UTC
          End Date: 2020-DEC-15 UTC
          Term Count: 5
      Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 10
  AP Perpetual Networkstack Advantage (DNA_NWStack):
    Description: AP Perpetual Network Stack entitled with DNA-A
    Total reserved count: 20
    Enforcement type: NOT ENFORCED
    Term information:
      Active: PID:C9800-CL-K9,SN:93BBAH93MGS
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 5
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
          Start Date: 2020-JUN-18 UTC
          End Date: 2020-DEC-15 UTC
          Term Count: 5
      Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 10

Purchased Licenses:
  No Purchase Information Available
```

# show license authorization

To display authorization-related information for (export-controlled and enforced) licenses, enter the **show license authorization** command in privileged EXEC mode.

**show license authorization**

## Syntax Description

| |
|---|
| This command has no keywords or arguments |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Amsterdam 17.3.2a | This command was introduced. |

## Usage Guidelines

Only export-controlled or enforced licenses require authorization before use.

While there are no export-controlled or enforced licenses on Cisco Catalyst Wireless Controllers, you can use this command to display migrated SLR authorization codes.

### Examples

See Table 14: show license authorization Field Descriptions, on page 846 for information about fields shown in the display.

See show license authorization Displaying Migrated Authorization Code, on page 848 for sample output.

*Table 14: show license authorization Field Descriptions*

<table>
<tr><th colspan="2">Field</th><th>Description</th></tr>
<tr><td rowspan="5">Overall Status</td><td colspan="2">Header for UDI information for all product instances in the set-up, the type of authorization that is installed, and configuration errors, if any.<br>In a High Availability set-up, all UDIs in the set-up are listed.</td></tr>
<tr><td>Active:<br>Status:</td><td>The active product instance UDI, followed by the status of the authorization code installation for this UDI.<br>If the status indicates that the authorization code is installed and there is a confirmation code, this is also displayed.</td></tr>
<tr><td>Standby:<br>Status:</td><td>The standby product instance UDI, followed by the status of the authorization code installation for this UDI.<br>If the status indicates that the authorization code is installed and there is a confirmation code, this is also displayed.</td></tr>
<tr><td>Member:<br>Status:</td><td>The member product instance UDI, followed by the status of the authorization code installation for this UDI.<br>If the status indicates that the authorization code is installed and there is a confirmation code, this is also displayed.</td></tr>
<tr><td>ERROR:</td><td>Configuration errors or discrepancies in the High Availability set-up, if any.</td></tr>
</table>

| Field | | Description |
|---|---|---|
| Authorizations | Header for detailed license authorization information. All licenses, their enforcement types, and validity durations are displayed. Errors are displayed for each product instance if its authorization or mode does not match what is installed on the active.<br>This section is displayed only if the product instance is using a license with an authorization code. | |
| | (): | License name and a shortened form of the license name. |
| | Description | License description. |
| | Total available count: | Total count of licenses that are available to consume.<br>This includes licenses of all durations (perpetual and subscription), including expired subscription licenses, for all the product instances in a High Availability setup. |
| | Enforcement type | Enforcement type for the license. This may be one of the following:<br>• Enforced<br>• Not enforced<br>• Export-Controlled |
| | Term information: | |

| Field | | Description |
|---|---|---|
| | | Header providing license duration information. The following fields maybe included under this header:<br>• Active: The active product instance UDI, followed by the status of the authorization code installation for this UDI.<br>• Authorization type: Type of authorization code installed and date of installation. The type can be: SLAC, UNIVERSAL, SPECIFIED, PAK, RTU.<br>• Start Date: Displays validity start date if the license is for a specific term or time period.<br>• Start Date: Displays validity end date if the license is for a specific term or time period.<br>• Term Count: License count.<br>• Subscription ID: Displays ID if the license is for a specific term or time period.<br>• License type: License duration. This can be: SUBSCRIPTION or PERPETUAL.<br>• Standby: The standby product instance UDI, followed by the status of the authorization code installation for this UDI.<br>• Member: The member product instance UDI, followed by the status of the authorization code installation for this UDI.<br>For more information about the duration or term of a license's validity, see <link tbd>. |
| Purchased Licenses | Header for license purchase information. | |
| | Active: | The active product instance and its the UDI. |
| | Count: | License count. |
| | Description: | License description. |
| | License type: | License duration. This can be: SUBSCRIPTION or PERPETUAL. |
| | Standby: | The standby product instance UDI. |
| | Member: | The member product instance UDI. |

### show license authorization Displaying Migrated Authorization Code

The following is sample output of the **show license authorization** command on a Cisco Catalyst 9800-CL Wireless Controller. The `Last Confirmation code:` shows that SLR authorization code is available after migration. Similar output is displayed on all supported Cisco Catalyst Wireless Controllers.

```
Device# show license authorization
Overall status:
  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
      Status: SPECIFIC INSTALLED on Nov 02 03:16:01 2020 IST
      Last Confirmation code: 102fc949
  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
      Status: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
      Last Confirmation code: ad4382fe

Specified license reservations:
  Aironet DNA Advantage Term Licenses (AIR-DNA-A):
    Description: DNA Advantage for Wireless
    Total reserved count: 20
    Enforcement type: NOT ENFORCED
    Term information:
      Active: PID:C9800-CL-K9,SN:93BBAH93MGS
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 5
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
          Start Date: 2020-JUN-18 UTC
          End Date: 2020-DEC-15 UTC
          Term Count: 5
      Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 10
  AP Perpetual Networkstack Advantage (DNA_NWStack):
    Description: AP Perpetual Network Stack entitled with DNA-A
    Total reserved count: 20
    Enforcement type: NOT ENFORCED
    Term information:
      Active: PID:C9800-CL-K9,SN:93BBAH93MGS
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 5
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
          Start Date: 2020-JUN-18 UTC
          End Date: 2020-DEC-15 UTC
          Term Count: 5
      Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 10

Purchased Licenses:
  No Purchase Information Available
```

# show license data conversion

To display license data conversion information, enter the **show license data** command in privileged EXEC mode.

**show license data conversion**

## Syntax Description

This command has no keywords or arguments

## Command Modes

Privileged EXEC (Device#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |
| Cisco IOS XE Amsterdam 17.3.2a | This command continues to be available with the introduction of Smart Licensing Using Policy. |

## Usage Guidelines

Although visible on the CLI, this command is not applicable to Cisco Catalyst Wireless Controllers.

# show license eventlog

To display event logs relating to Smart Licensing Using Policy, enter the **show license eventlog** command in privileged EXEC mode.

**show license eventlog** [ *days* ]

## Syntax Description

| | |
|---|---|
| *days* | Enter the number of days for which you want to display event logs. The valid value range is from 0 to 2147483647. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |
| Cisco IOS XE Amsterdam 17.3.2a | Additional events were added with the introduction of Smart Licensing Using Policy:<br>• Installation and removal of a policy<br>• Request, installation and removal of an authorization code.<br>• Installation and removal of a trust code.<br>• Addition of authorization source information for license usage. |

## Usage Guidelines

**Smart Licensing Using Policy**: If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2a or a later release, command output displays fields pertinent to Smart Licensing Using Policy.

**Smart Licensing**: If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing.

# show license history message

To display communication history between the product instance and CSSM or CSLU (as the case may be), enter the **show license history message** command in privileged EXEC mode. The output of this command is used by the technical support team, for troubleshooting.

**show license history message**

## Syntax Description

This command has no keywords or arguments.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Amsterdam 17.3.2a | This command was introduced. |

## Usage Guidelines

When you encounter an error message that you are not able to resolve, along with a copy of the message that appears on the console or in the system log, provide your Cisco technical support representative with sample output of these commands: **show license tech support**, **show license history message**, and the **show platform software sl-infra** privileged EXEC commands.

# show license reservation

To display license reservation information, enter the **show license reservation** command in privileged EXEC mode.

**show license reservation**

## Syntax Description

This command has no keywords or arguments

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |
| Cisco IOS XE Amsterdam 17.3.2a | This command continues to be available with the introduction of Smart Licensing Using Policy. |

## Usage Guidelines

The command continues to be available on the CLI and corresponding output is displayed, but with the introduction of Smart Licensing Using Policy, the notion of reservation is not longer applicable. Use the **show license all** command in privileged EXEC mode, to display *migrated* SLR licenses instead (the SLR authorization code is migrated to Smart Licensing Using Policy).

# show license status

To display information about licensing settings such as data privacy, policy, transport, usage reporting and trust codes, enter the **show license status** command in privileged EXEC mode.

**show license status**

## Syntax Description

| |
|---|
| This command has no keywords or arguments |

## Command Modes

Privileged EXEC (Device#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |
| Cisco IOS XE Amsterdam 17.3.2a | Command output was updated to reflect new fields that are applicable to Smart Licensing Using Policy. This includes `Trust code installed:`, `Policy in use`, `Policy name:` , reporting requirements as in the policy (`Attributes:` ), and fields related to usage reporting.<br>Command output no longer displays Smart Account and Virtual account information. |

## Usage Guidelines

**Smart Licensing**: If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing.

**Smart Licensing Using Policy**: If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2a or a later release, command output displays fields pertinent to Smart Licensing Using Policy.

### Examples

For information about the fields shown in the display, see Table 15: show license status Field Descriptions for Smart Licensing Using Policy, on page 855 .

For sample output, see:

- show license status with Cisco Default Policy (Smart Licensing Using Policy), on page 860
- show license status with Custom Policy (Smart Licensing Using Policy), on page 861

*Table 15: show license status Field Descriptions for Smart Licensing Using Policy*

| Field | | Description |
|---|---|---|
| Utility | Header for utility settings that are configured on the product instance. | |
| | Status: | Status |
| | Utility report: | Last attempt: |
| | Customer Information: | The following fields are displayed:<br>• Id:<br>• Name:<br>• Street<br>• City:<br>• State:<br>• Country:<br>• Postal Code: |
| Smart Licensing Using Policy: | Header for policy settings on the product instance. | |
| | Status: | Indicates if Smart Licensing Using Policy is enabled.<br>Smart Licensing Using Policy is supported starting from Cisco IOS XE Amsterdam 17.3.2 and is always enabled on supported software images. |
| Data Privacy: | Header for privacy settings that are configured on the product instance. | |
| | Sending Hostname: | A *yes* or *no* value which shows if the hostname is sent in usage reports. |
| | Callhome hostname privacy: | Indicates if the Call Home feature is configured as the mode of transport for reporting. If configured, one of these values is displayed:<br>• ENABLED<br>• DISABLED |
| | Smart Licensing hostname privacy: | One of these values is displayed:<br>• ENABLED<br>• DISABLED |
| | Version privacy: | One of these values is displayed:<br>• ENABLED<br>• DISABLED |

| Field | | Description |
|---|---|---|
| Transport: | Header for transport settings that are configured on the product instance. | |
| | Type: | Mode of transport that is in use.<br>Additional fields are displayed for certain transport modes. For example, if transport type is set to CSLU, the CSLU address is also displayed. |

| Field | | Description |
|---|---|---|
| Policy: | Header for policy information that is applicable to the product instance. | |
| | Policy in use: | Policy that is applied<br>This can be one of the following: Cisco default, Product default, Permanent License Reservation, Specific License Reservation, PAK license, Installed on <date>, Controller. |
| | Policy name: | Name of the policy |
| | Reporting ACK required: | A *yes* or *no* value which specifies if the report for this product instance requires CSSM acknowledgement (ACK) or not. The default policy is always set to "yes". |
| | Unenforced/Non-Export Perpetual Attributes | Displays policy values for perpetual licenses.<br>• First report requirement (days): The maximum amount of time available before the first report must be sent, followed by policy name.<br>• Reporting frequency (days): The maximum amount of time available before the subsequent report must be sent, followed by policy name.<br>• Report on change (days): he maximum amount of time available to send a report in case of a change in license usage, followed by policy name |
| | Unenforced/Non-Export Subscription Attributes | Displays policy values for subscription licenses.<br>• First report requirement (days): The maximum amount of time available before the first report must be sent, followed by policy name.<br>• Reporting frequency (days): The maximum amount of time available before the subsequent report must be sent, followed by policy name.<br>• Report on change (days): he maximum amount of time available to send a report in case of a change in license usage, followed by policy name |
| | Enforced (Perpetual/Subscription) License Attributes | |

| Field | | Description |
|---|---|---|
| | | Displays policy values for enforced licenses.<br>• First report requirement (days): The maximum amount of time available before the first report must be sent, followed by policy name.<br>• Reporting frequency (days): The maximum amount of time available before the subsequent report must be sent, followed by policy name.<br>• Report on change (days): The maximum amount of time available to send a report in case of a change in license usage, followed by policy name |
| | Export (Perpetual/Subscription) License Attributes | Displays policy values for export-controlled licenses.<br>• First report requirement (days): The maximum amount of time available before the first report must be sent, followed by policy name.<br>• Reporting frequency (days): The maximum amount of time available before the subsequent report must be sent, followed by policy name.<br>• Report on change (days): The maximum amount of time available to send a report in case of a change in license usage, followed by policy name |
| Miscellaneous | Header for custom ID. | |
| | Custom Id: | ID |

<table>
<tr><th colspan="2">Field</th><th>Description</th></tr>
<tr><td rowspan="9">Usage Reporting:</td><td colspan="2">Header for usage reporting (RUM reports) information.</td></tr>
<tr><td>Last ACK received:</td><td>Date and time of last ACK received, in the local time zone.</td></tr>
<tr><td>Next ACK deadline:</td><td>Date and time for next ACK. If the policy states that an ACK is not requires then this field displays `none`.<br>**Note** If an ACK is required and is not received by this deadline, a syslog is displayed.</td></tr>
<tr><td>Reporting Interval:</td><td>Reporting interval in days<br>The value displayed here depends on what you configure in the **license smart usage interval***interval_in_days* and the policy value. For more information, see the corresponding Syntax Description: license smart (global config), on page 381.</td></tr>
<tr><td>Next ACK push check:</td><td>Date and time when the product instance will submit the next polling request for an ACK. Date and time are in the local time zone.<br>This applies only to product instance- initiated communication to CSSM or CSLU. If the reporting interval is zero, or if no ACK polling is pending, then this field displays `none`.</td></tr>
<tr><td>Next report push:</td><td>Date and time when the product instance will send the next RUM report. Date and time are in the local time zone. If the reporting interval is zero, or if there are no pending RUM reports, then this field displays `none`.</td></tr>
<tr><td>Last report push:</td><td>Date and time for when the product instance sent the last RUM report. Date and time are in the local time zone.</td></tr>
<tr><td>Last report file write:</td><td>Date and time for when the product instance last saved an offline RUM report. Date and time are in the local time zone.</td></tr>
<tr><td>Last report pull:</td><td>Date and time for when usage reporting information was retrieved using data models. Date and time are in the local time zone.</td></tr>
</table>

<table>
<tr><th colspan="2">Field</th><th>Description</th></tr>
<tr><td rowspan="4">Trust Code Installed:</td><td colspan="2">Header for trust code-related information.<br>Displays date and time if trust code is installed. Date and time are in the local time zone.<br>If a trust code is not installed, then this field displays `none`.</td></tr>
<tr><td>Active:</td><td>Active product instance.<br>In a High Availability set-up, the the UDIs of all product instances in the set-up, along with corresponding trust code installation dates and times are displayed.</td></tr>
<tr><td>Standby:</td><td>Standby product instance.</td></tr>
<tr><td>Member:</td><td>Member product instance</td></tr>
</table>

### show license status with Cisco Default Policy (Smart Licensing Using Policy)

The following is sample output of the **show license status** command; a default is policy applied here.

```
Device# show license status

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license
  Proxy:
    Not Configured

Policy:
  Policy in use: Merged from multiple sources.
  Reporting ACK required: yes (CISCO default)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 365 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 90 (CISCO default)
    Reporting frequency (days): 90 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)

Miscellaneous:
  Custom Id: <empty>

Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: <none>
  Reporting push interval: 0 (no reporting)
  Next ACK push check: <none>
  Next report push: <none>
  Last report push: <none>
  Last report file write: <none>

Trust Code Installed: <none>
```

### show license status with Custom Policy (Smart Licensing Using Policy)

The following is sample output of the **show license status** command; a custom policy applied here.

```
Device# show license status
Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license
  Proxy:
    Not Configured

Policy:
  Policy in use: Installed On Nov 02 05:09:31 2020 IST
  Policy name: SLE Policy
  Reporting ACK required: yes (Customer Policy)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 60 (Customer Policy)
    Reporting frequency (days): 60 (Customer Policy)
    Report on change (days): 60 (Customer Policy)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 30 (Customer Policy)
    Reporting frequency (days): 30 (Customer Policy)
    Report on change (days): 30 (Customer Policy)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 90 (Customer Policy)
    Report on change (days): 90 (Customer Policy)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 90 (Customer Policy)
    Report on change (days): 90 (Customer Policy)

Miscellaneous:
  Custom Id: <empty>
```

```
Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: <none>
  Reporting push interval: 0 (no reporting)
  Next ACK push check: <none>
  Next report push: <none>
  Last report push: <none>
  Last report file write: <none>

Trust Code Installed:
  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
    INSTALLED on Nov 02 05:09:31 2020 IST
  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
    INSTALLED on Nov 02 05:09:31 2020 IST
```

# show license summary

To display a brief summary of license usage, which includes information about licenses being used, the count, and status, enter the **show license summary** command in privileged EXEC mode.

**show license summary**

## Syntax Description

| |
|---|
| This command has no keywords or arguments |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |
| Cisco IOS XE Amsterdam 17.3.2a | Command output was updated to reflect valid license status for Smart Licensing Using Policy. Valid license statuses include: `IN USE`, `NOT IN USE`, `NOT AUTHORIZED`.<br>Command output was also updated to remove registration and authorization information.<br>Command output no longer displays Smart Account and Virtual account information. |

## Usage Guidelines

**Smart Licensing**: If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing.

**Smart Licensing Using Policy**: If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2a or a later release, command output displays fields pertinent to Smart Licensing Using Policy.

The licenses on Cisco Catalyst Wireless Controllers are never `NOT AUTHORIZED`, because none of the available licenses are export-controlled or enforced (Only these licenses require authorization before use).

### Examples

See Table 16: show license summary Field Descriptions, on page 863 for information about fields shown in the display.

#unique_661 unique_661_Connect_42_section_tzb_tyb_4nb

show license summary: NOT IN USE (Smart Licensing Using Policy), on page 864

*Table 16: show license summary Field Descriptions*

| Field | Description |
|---|---|
| License | Name of the licenses in use |
| Entitlement Tag | Short name for license |
| Count | License count |

| Field | Description |
|---|---|
| Status | License status can be one of the following<br>• In-Use: Valid license, and in-use.<br>• Not In-Use<br>• Not Authorized: Means that the license requires installation of SLAC before use. |

### show license summary: NOT IN USE (Smart Licensing Using Policy)

The following is sample output of the **show license summary** command, where no APs have joined the controller. Current consumption (Count) is therefore zero, and the `Status` field shows that the licenses are `NOT IN USE`:

```
Device# show license summary

Device#show license summary
License Reservation is ENABLED

License Usage:
  License                 Entitlement Tag               Count Status
  -----------------------------------------------------------------------------
  Aironet DNA Advantag... (AIR-DNA-A)                       0 NOT IN USE
  AP Perpetual Network... (DNA_NWStack)                     0 NOT IN USE
```

# show license tech

To display licensing information to help the technical support team to solve a problem, enter the **show license tech** command in privileged EXEC mode. The output for this command includes outputs of several other **show license** commands and more.

**show license tech** { **data** { **conversion** } | **eventlog** [ *days* ] | **reservation** | **support** }

## Syntax Description

| | |
|---|---|
| **data** { **conversion** } | Displays license data conversion information. |
| **eventlog** [ *days* ] | Displays event logs related to Smart Licensing Using Policy.<br>For *days*, enter the number of days for which you want to display event logs. The valid value range is from 0 to 2147483647. |
| **reservation** | Displays license reservation information. |
| **support** | Displays licensing information that helps the technical support team to debug a problem. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |
| Cisco IOS XE Amsterdam 17.3.2a | Command output was updated to reflect new fields that are applicable to Smart Licensing Using Policy. |

## Usage Guidelines

**Smart Licensing**: If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing (whether smart licensing is enabled, all associated licensing certificates, compliance status, and so on).

**Smart Licensing Using Policy**: If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2 or a later release, command output displays fields pertinent to Smart Licensing Using Policy. Note the following guidelines:

When you encounter an error message that you are not able to resolve, along with a copy of the message that appears on the console or in the system log, provide your Cisco technical support representative with sample output of these commands: **show license tech support**, **show license history message**, and the **show platform software sl-infra all** privileged EXEC commands.

### Example (Smart Licensing Using Policy)

The following is sample output from the **show license tech support** command.

```
Device# show license tech support

Smart Licensing Tech Support info

Smart Licensing Status
======================
Smart Licensing is ENABLED
License Reservation is ENABLED

Registration:
  Status: REGISTERED - SPECIFIC LICENSE RESERVATION
  Export-Controlled Functionality: ALLOWED
  Initial Registration: SUCCEEDED on Nov 02 03:16:01 2020 IST

License Authorization:
  Status: AUTHORIZED - RESERVED on Nov 02 03:16:01 2020 IST

Export Authorization Key:
  Features Authorized:
    <none>

Utility:
  Status: DISABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license

Evaluation Period:
  Evaluation Mode: Not In Use
  Evaluation Period Remaining: 89 days, 23 hours, 42 minutes, 47 seconds

License Usage
=============
Handle: 1
  License: AP Perpetual Networkstack Advantage
  Entitlement tag:
regid.2018-06.com.cisco.DNA_NWStack,1.0_e7244e71-3ad5-4608-8bf0-d12f67c80896
  Description: AP Perpetual Network Stack entitled with DNA-A
  Count: 1
  Version: 1.0
  Status: AUTHORIZED(3)
  Status time: Nov 02 03:16:01 2020 IST
  Request Time: Nov 02 02:55:34 2020 IST
  Export status: NOT RESTRICTED
  Soft Enforced: True

Handle: 2
  License: Aironet DNA Advantage Term Licenses
  Entitlement tag: regid.2017-08.com.cisco.AIR-DNA-A,1.0_b6308627-3ab0-4a11-a3d9-586911a0d790

  Description: DNA Advantage for Wireless
  Count: 1
  Version: 1.0
  Status: AUTHORIZED(3)
  Status time: Nov 02 03:16:01 2020 IST
  Request Time: Nov 02 02:55:34 2020 IST
  Export status: NOT RESTRICTED
  Soft Enforced: True

Product Information
===================
UDI: PID:C9800-CL-K9,SN:93BBAH93MGS
```

```
HA UDI List:
    Active:PID:C9800-CL-K9,SN:93BBAH93MGS
    Standby:PID:C9800-CL-K9,SN:9XECPSUU4XN

Agent Version
=============
Smart Agent for Licensing: 4.8.7_rel/52

Upcoming Scheduled Jobs
=======================
Current time: Nov 02 03:17:23 2020 IST
Daily: Nov 03 02:47:04 2020 IST (23 hours, 29 minutes, 41 seconds remaining)
Certificate Renewal: Not Available
Certificate Expiration Check: Not Available
Authorization Renewal: Not Available
Authorization Expiration Check: Not Available
Init Flag Check: Not Available
Evaluation Expiration Check: Not Available
Ack Expiration Check: Not Available
Evaluation Expiration Warning: Not Available
IdCert Expiration Warning: Not Available
Reservation request in progress warning: Not Available
Reservation configuration mismatch between nodes in HA mode: Nov 09 03:16:30 2020 IST (6
days, 23 hours, 59 minutes, 7 seconds remaining)
Endpoint Report Request: Not Available

License Certificates
====================
Production Cert: True
Not registered. No certificates installed

HA Info
==========
RP Role: Active
Chassis Role: Active
Behavior Role: Active
RMF: True
CF: True
CF State: Stateless
Message Flow Allowed: False

Reservation Info
================
License reservation: ENABLED

Overall status:
  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
      Reservation status: SPECIFIC INSTALLED on Nov 02 03:16:01 2020 IST
      Export-Controlled Functionality: ALLOWED
      Request code: <none>
      Last return code: <none>
      Last Confirmation code: 102fc949
      Reservation authorization code:
<specificPLR><authorizationCode><flag>A</flag><version>C</version><piid>[illegible]</piid><timestamp>[illegible]</timestamp><entitlements><entitlement><tag>regid.2017-08.com.cisco.AIR-DNA-A,1.0_b6308627-3ab0-4a11-a3d9-586911a0d790</tag><count>5</count><startDate>2020-Oct-14
 UTC</startDate><endDate>2021-Apr-12
UTC</endDate><licenseType>TERM</licenseType><displayName>Aironet DNA Advantage Term
Licenses</displayName><tagDescription>DNA Advantage for
Wireless</tagDescription><subscriptionID></subscriptionID></entitlement><entitlement><tag>regid.2017-08.com.cisco.AIR-DNA-A,1.0_b6308627-3ab0-4a11-a3d9-586911a0d790</tag><count>5</count><startDate>2020-Jun-18
 UTC</startDate><endDate>2020-Dec-15
UTC</endDate><licenseType>TERM</licenseType><displayName>Aironet DNA Advantage Term
Licenses</displayName><tagDescription>DNA Advantage for
Wireless</tagDescription><subscriptionID></subscriptionID></entitlement><entitlement><tag>regid.2018-06.com.cisco.DNA_NWStack,1.0_e7244e71-3ad5-4608-8bf0-d12f67c80896</tag><count>5</count><startDate>2020-Oct-14
 UTC</startDate><endDate>2021-Apr-12
UTC</endDate><licenseType>TERM</licenseType><displayName>AP Perpetual Networkstack
```

```
Advantage</displayName><tagDescription>AP Perpetual Network Stack entitled with
DNA-A</tagDescription><subscriptionID></subscriptionID></entitlement><entitlement><tag>regid.2018-06.com.cisco.DNA_NWStack,1.0_[illegible]</tag><count>5</count><startDate>2020-Jun-18
 UTC</startDate><endDate>2020-Dec-15
UTC</endDate><licenseType>TERM</licenseType><displayName>AP Perpetual Networkstack
Advantage</displayName><tagDescription>AP Perpetual Network Stack entitled with
DNA-A</tagDescription><subscriptionID></subscriptionID></entitlement></entitlements></authorizationCode><signature>[illegible]</signature><udi>P:C9800-CL-K9,S:93BBAH93MGS</udi></specificPLR>

  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
      Reservation status: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
      Export-Controlled Functionality: ALLOWED
      Request code: <none>
      Last return code: <none>
      Last Confirmation code: ad4382fe
      Reservation authorization code:
<specificPLR><authorizationCode><flag>A</flag><version>C</version><piid>[illegible]</piid><timestamp>[illegible]</timestamp><entitlements><entitlement><tag>regid.2018-06.com.cisco.DNA_NWStack,1.0_[illegible]</tag><count>10</count><startDate>2020-Oct-14
 UTC</startDate><endDate>2021-Apr-12
UTC</endDate><licenseType>TERM</licenseType><displayName>AP Perpetual Networkstack
Advantage</displayName><tagDescription>AP Perpetual Network Stack entitled with
DNA-A</tagDescription><subscriptionID></subscriptionID></entitlement><entitlement><tag>regid.2017-08.com.cisco.AIR-DNA-A,1.0_[illegible]</tag><count>10</count><startDate>2020-Oct-14
 UTC</startDate><endDate>2021-Apr-12
UTC</endDate><licenseType>TERM</licenseType><displayName>Aironet DNA Advantage Term
Licenses</displayName><tagDescription>DNA Advantage for
Wireless</tagDescription><subscriptionID></subscriptionID></entitlement></entitlements></authorizationCode><signature>[illegible]</signature><udi>P:C9800-CL-K9,S:9XECPSUU4XN</udi></specificPLR>

Specified license reservations:
  Aironet DNA Advantage Term Licenses (AIR-DNA-A):
    Description: DNA Advantage for Wireless
    Total reserved count: 20
    Term information:
      Active: PID:C9800-CL-K9,SN:93BBAH93MGS
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 5
          Subscription ID: <none>
        License type: TERM
          Start Date: 2020-JUN-18 UTC
          End Date: 2020-DEC-15 UTC
          Term Count: 5
          Subscription ID: <none>
      Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 10
          Subscription ID: <none>
  AP Perpetual Networkstack Advantage (DNA_NWStack):
    Description: AP Perpetual Network Stack entitled with DNA-A
    Total reserved count: 20
    Term information:
      Active: PID:C9800-CL-K9,SN:93BBAH93MGS
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 5
          Subscription ID: <none>
        License type: TERM
          Start Date: 2020-JUN-18 UTC
          End Date: 2020-DEC-15 UTC
          Term Count: 5
          Subscription ID: <none>
      Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 10
          Subscription ID: <none>

Other Info
==========
Software ID: regid.2018-05.com.cisco.WLC_9500C,1.0_85665885-b865-4e32-8184-5510412fcb54
Agent State: authorized
TS enable: True
Transport: Smart
  Default URL: https://smartreceiver.cisco.com/licservice/license
Locale: en_US.UTF-8
Debug flags: 0x7
Privacy Send Hostname: True
Privacy Send IP: True
Build type:: Production
sizeof(char)  : 1
sizeof(int)   : 4
sizeof(long)  : 4
sizeof(char *): 8
sizeof(time_t): 4
sizeof(size_t): 8
Endian: Big
Write Erase Occurred: False
XOS version: 0.12.0.0
Config Persist Received: False
Message Version: 1.3
connect_info.name: <empty>
connect_info.version: <empty>
connect_info.additional: <empty>
connect_info.prod: False
connect_info.capabilities: <empty>
agent.capabilities: UTILITY, DLC, AppHA, MULTITIER, EXPORT_2, OK_TRY_AGAIN
SmartAgentClientWaitForServer: 2000
SmartAgentCmReTrySend: True
SmartAgentClientIsUnified: True
SmartAgentCmClient: True
SmartAgentClientName: UnifiedClient
builtInEncryption: True
enableOnInit: True
routingReadyByEvent: True
systemInitByEvent: True
SmartAgentFederalLicense: True
SmartAgent_Crypto_Exit_CB: 0x55B353357A20
SmartAgent_Crypto_Start_CB: 0x55B353357A10
SmartAgentMultiTenant: False
attr365DayEvalSyslog: True
checkPointWriteOnly: False
SmartAgentDelayCertValidation: False
enableByDefault: False
conversionAutomatic: True
conversionAllowed: False
storageEncryptDisable: False
storageLoadUnencryptedDisable: False
TSPluginDisable: False
bypassUDICheck: False
loggingAddTStamp: False
loggingAddTid: True
platformOverrideEvent: UnknownPlatformEvent
WaitForHaRole: False
standbyIsHot: True
chkPtType: 2
delayCommInit: False
roleByEvent: True
```

```
maxTraceLength: 150
traceAlwaysOn: True
debugFlags: 0
Event log max size: 5120 KB
Event log current size: 21 KB

Platform Provided Mapping Table
===============================
<empty>
```

# show license udi

To display Unique Device Identifier (UDI) information for a product instance, enter the **show license udi** command in privileged EXEC mode. In a High Availability set-up, the output displays UDI information for all connected product instances.

**show license udi**

## Syntax Description

This command has no keywords or arguments

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |
| Cisco IOS XE Amsterdam 17.3.2a | This command continues to be available with the introduction of Smart Licensing Using Policy. |

## Usage Guidelines

**Smart Licensing Using Policy**: If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2a or a later release, command output displays fields pertinent to Smart Licensing Using Policy.

**Smart Licensing**: If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing.

### Examples

show license udi with Standalone Product Instance, on page 871

show license udi with Active and Standby, on page 871

### show license udi with Standalone Product Instance

The following is sample output from the **show license udi** command on a standalone product instance.

```
Device# show license udi

UDI: PID:C9800-L-F-K9,SN:FCW2323W016
```

### show license udi with Active and Standby

The following is sample output from the **show license udi** command in a High Availability set-up where an active and a standby product instances exist. UDI information is displayed for both.

```
Device# show license udi

UDI: PID:C9800-CL-K9,SN:93BBAH93MGS

HA UDI List:
    Active:PID:C9800-CL-K9,SN:93BBAH93MGS
    Standby:PID:C9800-CL-K9,SN:9XECPSUU4XN
```

# show license usage

To display license usage information such as status, a count of licenses being used, and enforcement type, enter the **show license usage** command in privileged EXEC mode.

**show license usage**

### Syntax Description

| This command has no keywords or arguments |
|---|

### Command Modes

Privileged EXEC

### Command History

| Release | Modification |
|---|---|
| This command was introduced in a release earlier than Cisco IOS XE Amsterdam 17.3.2 | This command was introduced. |
| Cisco IOS XE Amsterdam 17.3.2a | Command output was updated to reflect new fields that are applicable to Smart Licensing Using Policy. This includes the `Status`, `Enforcement type` fields.<br>Command output was also updated to remove reservation related information, authorization status information, and export status information. |

### Usage Guidelines

**Smart Licensing Using Policy**: If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2a or a later release, command output displays fields pertinent to Smart Licensing Using Policy.

**Smart Licensing**: If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing.

### Examples

See Table 17: show license usage Field Descriptions, on page 872 for information about fields shown in the display.

show license usage with unenforced licenses (Smart Licensing Using Policy), on page 873

show license usage with unenforced SLR licenses (Smart Licensing Using Policy), on page 874

*Table 17: show license usage Field Descriptions*

| Field | Description |
|---|---|
| License Authorization:<br>Status: | Displays overall authorization status. |
| (): | Name of the license as in CSSM.<br>If this license is one that requires an authorization code, the name of the li the code. |

| Field | Description |
|---|---|
| Description | Description of the license as in CSSM. |
| Count | License count. If the license is not in-use, the count is reflected as ze |
| Version | Version. |
| Status | License status can be one of the following<br>• In-Use: Valid license, and in-use.<br>• Not In-Use<br>• Not Authorized: Means that the license requires installation of S more information, see |
| Export Status: | Indicates if this license is export-controlled or not. Accordingly, one of is displayed:<br>• RESTRICTED - ALLOWED<br>• RESTRICTED - NOT ALLOWED<br>• NOT RESTRICTED |
| Feature name | Name of the feature that uses this license. |
| Feature Description: | Description of the feature that uses this license. |
| Utility Subscription id: | ID<br>Not applicable, because the corresponding confiuration option is not |
| Enforcement type | Enforcement type status for the license. This may be one of the follo<br>• ENFORCED<br>• NOT ENFORCED<br>• EXPORT RESTRICTED - ALLOWED<br>• EXPORT RESTRICTED - NOT ALLOWED<br>For more information about enforcement types, see <link tbd> |

### show license usage with unenforced licenses (Smart Licensing Using Policy)

The following is sample output of the **show license usage** command. Unenforced licenses are in-use here.

```
Device# show license usage

License Authorization:
  Status: Not Applicable

air-network-essentials (DNA_NWSTACK_E):
  Description: air-network-essentials
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: air-network-essentials
  Feature Description: air-network-essentials
  Enforcement type: NOT ENFORCED
  License type: Perpetual

air-dna-essentials (AIR-DNA-E):
  Description: air-dna-essentials
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: air-dna-essentials
  Feature Description: air-dna-essentials
  Enforcement type: NOT ENFORCED
  License type: Perpetual
```

### show license usage with unenforced SLR licenses (Smart Licensing Using Policy)

The following is sample output of the **show license usage** command. Migrated SLR licenses are in-use here:

```
Device# show license usage

air-network-advantage (DNA_NWStack):
  Description: air-network-advantage
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: air-network-advantage
  Feature Description: air-network-advantage
  Enforcement type: NOT ENFORCED
  License type: Perpetual
  Reservation:
    Reservation status: SPECIFIC INSTALLED
    Total reserved count: 20

air-dna-advantage (AIR-DNA-A):
  Description: air-dna-advantage
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: air-dna-advantage
  Feature Description: air-dna-advantage
  Enforcement type: NOT ENFORCED
  License type: Perpetual
  Reservation:
    Reservation status: SPECIFIC INSTALLED
    Total reserved count: 20
```

# show platform software sl-infra

To display troubleshooting information and for debugging, enter the **show platform software sl-infra** command in privileged EXEC mode. The output of this command is used by the technical support team, for troubleshooting and debugging.

**show platform software sl-infra** { **all** | **current** | **debug** | **stored** }

## Syntax Description

| | |
|---|---|
| **all** | Displays current, debugging, and stored information. |
| **current** | Displays current license-related information. |
| **debug** | Enables debugging |
| **stored** | Displays information that is stored on the product instance. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Amsterdam 17.3.2a | This command was introduced. |

## Usage Guidelines

When you encounter an error message that you are not able to resolve, along with a copy of the message that appears on the console or in the system log, provide your Cisco technical support representative with sample output of these commands: **show license tech support**, **show license history message**, and the **show platform software sl-infra all** privileged EXEC commands.

# show platform software tls client summary

To view the TLS client summary details, use the **show platform software tls client summary** command.

**show platform software tls client summary**

## Syntax Description

This command has no keywords or arguments.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Bengaluru 17.6.1 | This command was introduced. |

## Examples

This example shows how to view the TLS client summary details:

```
Device # show platform software tls client summary

Name     ID     Gateway    Port   Auth     Trustpoint   DPD Time Rekey Time  Retry Time
---------------------------------------------------------------------------------------
fqdn     0                 8443   PSK       N/A           60       300         20
```

# show platform software client detail

To display a summary of TLS client session detail, session statistics, tunnel statistics, and DNS counters, use the **show platform software client detail** command.

**show platform software client detail**

## Syntax Description

This command has no keywords or arguments.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Bengaluru 17.6.1 | This command was introduced. |

## Examples

This example shows how to view the TLS client summary details:

```
Device # show platform software client detail

TLS Client           : Session Detail
Session Name         : fqdn
FQDN resolved IP     : 10.194.234.149
ID                   : 0
Created              : 04/20/21 00:36:42
Updated              : 04/22/21 05:56:03
State                : Up (Rekey)
Up Time              : 04/21/21 20:30:21 ( 9 hours 25 minutes 45 seconds )
Down Time            : 04/21/21 20:30:01
Rekey Time           : 04/22/21 05:55:51 ( 15 seconds )

TLS Session Statistics

Up Notifications     : 3
Down Notifications   : 2
Rekey Notifications  : 636
DP State Updates     : 0
DPD Cleanups         : 0

Packets From     Packets To  Packet Errors To     Bytes From           Bytes To
---------------------------------------------------------------------------------
  BinOS              80          0                                         0
  IOSd                0          0                    0                    0

  TLS Client          0          0                    0                    0


TLS Tunnel Statistics
Type            Tx Packets      Rx Packets
-------------------------------------------
  Total             0               80
  CSTP Ctrl      3836             3836
  CSTP Data        80                0

Type            Requests         Responses
--------------------------------------------
```

```
CSTP Cfg          639                  639
CSTP DPD         3197                 3197

Invalid CSTP Rx          : 0
Injected Packet Success  : 0
Injected Packet Failed   : 0
Consumed Packets         : 0

TLS Tunnel DNS Counters
DNS Resolve Request Success Count    : 641
DNS Resolve Request Failure Count    :  0
DNS Resolve Success Count            : 639
DNS Resolve Failure Count            :  2
```

# show platform software tls statistics

To view the TLS client global statistic details, use the **show platform software tls statistics** command.

**show platform software tls statistics**

## Syntax Description

This command has no keywords or arguments.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Bengaluru 17.6.1 | This command was introduced. |

## Examples

This example shows how to view the TLS client summary details:

```
Device # show platform software tls statistics

TLS Client - Global Statistics
Session Statistics
Up/Down           : 5/2
Rekeys            : 636
DP Updates        :   0
DPD Cleanups      :   0

Packets From    Packets To   Packet Errors To     Bytes From   Bytes To
----------------------------------------------------------------------
BinOS              85             0                  0             0
IOSd 0             0              0                  0             0
TLS Client  0      0                                 0             0

Tunnel Statistics
SSL Handshake Init/Done     : 641/641
TCP Connection Req/Done     : 641/641

Tunnel Packets
Rx/Tx                       : 85/0
Injected / Failed           : 0/0
Consumed                    :  0

CSTP Packets
Control Rx/Tx               : 3839 / 3839
Data Rx/Tx                  : 0 / 85
Config Req/Resp             : 641 / 641
DPD Req/Resp                : 3198 / 3198
Invalid Rx                  : 0

FQDN Counters
Req/Resp/Success            : 0/0/0

NAT Counters
Transalte In/Out            : 0/0
Ignore    In/Out            : 0/0
Failed                      : 0
Invalid                     : 0
```

```
No Entry                    : 0
Unsupported                 : 0

Internal Counters
Type           Allocated            Freed
-------------------------------------------------
EV              1299                 1295
Tunnel           5                    4
Conn            643                  642
Sess             3                    2

Config Message Related Counters
Type               Success              Failed
-------------------------------------------------
Create                3                    0
Delete                2                    0
```

# show platform software tls session summary

To view the tls client session summary, use the **show platform software tls session summary** command.

**show platform software tls session summary**

## Syntax Description

This command has no keywords or arguments.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Bengaluru 17.6.1 | This command was introduced. |

## Examples

This example shows how to view the TLS client summary details:

```
Device # show platform software tls session summary

TLS Client - Session Summary
Name     ID      Created            State    Since               Elapsed
------------------------------------------------------------------------------------------
fqdn     0     04/20/21 00:36:42    Up     04/21/21 20:30:21   9 hours 26 minutes 44 seconds
```

# show lisp site detail

To see detailed Locator ID Separation Protocol (LISP) site information on a map server, use the **show lisp site detail** command.

**show lisp site detail** [**eid-table** {**default** | **vlan** *vlan-id* | **vrf** *vrf-name* } | **instance-id** *id-number* | **internal** {**eid-table** {**default** | **vlan** *vlan-id* | **vrf** *vrf-name*} | **instance-id** *id-number*}]

## Syntax Description

| | |
|---|---|
| **eid-table** | Option to enter the EID table. |
| **default** | Shows the information for the default VRF. |
| **vlan** *vlan-id* | Enter the VLAN information. |
| **vrf** *vrf-name* | Enter the VRF name. |
| **instance-id** *id-number* | Enter the EID instance ID. |
| **internal** | Shows the site's detailed internal information. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see detailed Locator ID Separation Protocol (LISP) site information on a map server:

```
Device# show lisp site detail
```

# show logging profile wireless end timestamp

To specify log filtering end location timestamp for filtering, use the **show logging profile wireless end timestamp** command.

**show logging profile wireless end timestamp** *time-stamp*

## Syntax Description

| | |
|---|---|
| *time-stamp* | Time to end the filtering. For example, 2017/02/10 14:41:50.849. |

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

Ensure that you enable internal keyword using the **show logging profile wireless internal** command to get the trace output.

### Example

The following example shows how to specify log filtering end location timestamp for filtering:

```
Device# show logging profile wireless end timestamp 2017/02/10 14:41:50.849
```

# show logging profile wireless filter

To specify filter for logs, use the **show logging profile wireless filter** command.

**show logging profile wireless filter** {**ipv4** | **mac** | **string** | **uuid**}

## Syntax Description

| | |
|---|---|
| **ipv4** | Selects logs with specific IP address app context. |
| **mac** | Selects logs with specific MAC app context. |
| **string** | Selects logs with specific string app context. |
| **uuid** | Selects logs with specific Universally Unique Identifier (UUID) app context. |

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

Ensure that you enable **internal** keyword using the **show logging profile wireless internal** command to get the trace output.

Without the **internal** keyword, only customer curated logs are displayed.

### Example

The following example shows how to specify filter for logs:

```
Device# show logging profile wireless filter ipv4 10.10.11.1
```

# show logging profile wireless fru

To specify field-replaceable unit (FRU) specific commands, use the **show logging profile wireless fru** command.

**show logging profile wireless fru {0 {reverse | to-file}| chassis}** {**0** {**reverse** | **to-file**} | **chassis**}

## Syntax Description

| | |
|---|---|
| **0** | SPA-Inter-Processor slot 0. |
| **reverse** | Shows logs in reverse chronological order. |
| **to-file** | Decodes files stored in disk and write output to file. |
| **chassis** | Chassis name. |

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

Ensure that you enable **internal** keyword using the **show logging profile wireless internal** command to get the trace output.

Without the **internal** keyword, only customer curated logs are displayed.

### Example

The following example shows how to specify FRU specific commands:

```
Device# show logging profile wireless fru 0
```

# show logging profile wireless internal

To select all the logs, use the **show logging profile wireless internal** command.

**show logging profile wireless internal**

## Syntax Description

This command has no keywords or arguments.

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

Ensure that you enable **internal** keyword using the **show logging profile wireless internal** command to get the trace output.

Without the **internal** keyword, only customer curated logs are displayed.

### Example

The following example shows how to display all the logs:

```
Device# show logging profile wireless internal
```

# show logging profile wireless level

To select logs above a specific level, use the **show logging profile wireless level** command.

**show logging profile wireless level** { **debug** | **emergency** | **error** | **info** | **noise** | **notice** | **verbose** | **warning** }

## Syntax Description

| | |
|---|---|
| **debug** | Selects debug messages. |
| **emergency** | Selects emergency possible messags. |
| **error** | Selects error messages. |
| **info** | Selects informational messages. |
| **noise** | Selects maximum possible messages. |
| **notice** | Selects notice messages. |
| **verbose** | Selects verbose debug messages. |
| **warning** | Selects warning messages. |

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

Ensure that you enable **internal** keyword using the **show logging profile wireless internal** command to get the trace output.

Without the **internal** keyword, only customer curated logs are displayed.

### Example

The following example shows how to select logs above a specific level:

```
Device# show logging profile wireless level info
```

# show logging profile wireless module

To select logs for specific modules, use the **show logging profile wireless module** command.

**show logging profile wireless module** *module-name*

## Syntax Description

| | |
|---|---|
| *module-name* | A comma or space separated list of module names. For example, dbal, tdllib or "dbal tdllib". |

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

Ensure that you enable **internal** keyword using the **show logging profile wireless internal** command to get the trace output.

Without the **internal** keyword, only customer curated logs are displayed.

### Example

The following example shows how to select logs for specific modules:

```
Device# show logging profile wireless module dbal
```

# show logging profile wireless reverse

To view logs in reverse chronological order, use the **show logging profile wireless reverse** command.

**show logging profile wireless reverse**

## Syntax Description

This command has no keywords or arguments.

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

Ensure that you enable **internal** keyword using the **show logging profile wireless internal** command to get the trace output.

Without the **internal** keyword, only customer curated logs are displayed.

### Example

The following example shows how to view logs in reverse chronological order:

```
Device# show logging profile wireless reverse
```

# show logging profile wireless start

To specify log filtering start location, use the **show logging profile wireless start** command.

**show logging profile wireless start** {**marker** *marker* | **timestamp** *time-stamp*}

## Syntax Description

| | |
|---|---|
| **marker** | The marker to start filtering from. It must match with previously set marker. |
| **timestamp** | The timestamp for filtering. for example, "2017/02/10 14:41:50.849". |

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

Ensure that you enable **internal** keyword using the **show logging profile wireless internal** command to get the trace output.

Without the **internal** keyword, only customer curated logs are displayed.

### Example

The following example shows how to specify log filtering start location:

```
Device# show logging profile wireless start timestamp 2017/02/10 14:41:50.849
```

# show logging profile wireless switch

To specify the switch to look for logs, use the **show logging profile wireless switch** command.

**show logging profile wireless switch** {*switch-num* | **active** | **standby**}

## Syntax Description

| | |
|---|---|
| *chassis-num* | Chassis number. |
| **active** | Selects the active instance. |
| **standby** | Selects the standby instance. |

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

Ensure that you enable **internal** keyword using the **show logging profile wireless internal** command to get the trace output.

Without the **internal** keyword, only customer curated logs are displayed.

### Example

The following example shows how to specify the chassis number to look for logs:

```
Device# show logging profile wireless switch active
```

# show logging profile wireless to-file

To decode files stored in disk and write the output to a file, use the **show logging profile wireless to-file** command.

**show logging profile wireless to-file** *output-file-name*

## Syntax Description

| | |
|---|---|
| *output-file-name* | Output file name. File with this name will be created in the flash memory. |

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

Ensure that you enable **internal** keyword using the **show logging profile wireless internal** command to get the trace output.

Without the **internal** keyword, only customer curated logs are displayed.

### Example

The following example shows how to decode files stored in disk and write the output to a file:

```
Device# show logging profile wireless to-file testfile
```

# show mobility

To display information about the Layer 3 mobility and the wireless network, use the **showmobility** command in privileged EXEC mode.

**show mobility** {**ap** [*ip-address*] | **mn** [**ip** *ip-address*] | **mac** *mac-address* | **network** *network-id* | **status**}

## Syntax Description

| | |
|---|---|
| **ap** | Displays information about the access point. |
| *ip-address* | (Optional) IP address. |
| **mn** | Displays information about the mobile node. |
| **ip** *ip-address* | (Optional) Displays information about the IP database thread. |
| **mac** *mac-address* | Displays information about the MAC database thread. |
| **network** *network-id* | Displays information for a specific wireless network ID. |
| **status** | Displays status information. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(18)SXD | This command was introduced on the Supervisor Engine 720. |
| 12.2(18)SXD3 | The output of this command was changed to include the TCP adjust-mss status. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

This command is supported on Cisco 7600 series routers that are configured with a WLSM only.

## Examples

This example shows how to display information about the access point:

```
Router# show mobility
 ap
AP IP Address   AP Mac Address Wireless Network-ID
--------------- -------------- -------------------
10.1.1.2 000d.29a2.a852 101 102 109 103
```

This example shows how to display information about the access points for a specific network ID:

```
Router# show mobility
 ap 172.16.1.2 detail
IP Address : 172.16.1.2
MAC Address : 000d.29a2.a852
Participating Wireless Tunnels: 101, 102, 109, 103
Registered Mobile Nodes on AP {172.16.1.2, 000d.29a2.a852} :
MN Mac Address MN IP Address AP IP Address Wireless Network-ID
-------------- --------------- --------------- -------------------
000a.8afa.85c9 10.1.3.11 172.16.1.2 103
```

```
000d.bdb7.83f7 10.1.2.11 172.16.1.2 102
000d.bdb7.83fb 10.1.1.11 172.16.1.2 101
Router# show mobility
 network-id 101
Wireless Network ID : 101
Wireless Tunnel Source IP Address : 10.1.1.1
Wireless Network Properties : Trusted
Wireless Network State : Up
Registered Access Point on Wireless Network 101:
AP IP Address AP Mac Address Wireless Network-ID
--------------- -------------- -------------------
176.16.1.2 000d.29a2.a852 101 102 109 103
Registered Mobile Nodes on Wireless Network 101:
MN Mac Address MN IP Address AP IP Address Wireless Network-ID
-------------- --------------- --------------- -------------------
000d.bdb7.83fb 10.1.1.11 176.16.1.2 101
Router# show mobility
 status
WLAN Module is located in Slot: 4 (HSRP State: Active) LCP
Communication status      : up
MAC address used for Proxy ARP: 0030.a349.d800
Number of Wireless Tunnels    : 1
Number of Access Points       : 2
Number of Mobile Nodes        : 0
Wireless Tunnel Bindings:
Src IP Address   Wireless Network-ID  Flags
---------------  -------------------  -------
10.1.1.1          101                  B
Flags: T=Trusted, B=IP Broadcast enabled, A=TCP Adjust-mss enabled
```

## Related Commands

| Command | Description |
|---|---|
| **mobility** | Configures the wireless mGRE tunnels. |

# show monitor capture

To display the contents of a monitor capture buffer or a capture point, use the **show monitor capture** command in privileged EXEC mode.

**show monitor capture** [ *epc-capture-name* [ **parameter** | **buffer** [ **brief** | **detailed** | **dump** ] ] ]

## Syntax Description

| | |
|---|---|
| *epc-capture-name* | Specifies the name of the embedded packet capture. |
| **buffer** | Displays the contents of the specified capture buffer. |
| **dump** | (Optional) Displays a hexadecimal dump of the captured packet in addition to the metadata. |
| **brief** | (Optional) Provides a brief output of the captured packet information. |
| **detail** | (Optional) Provides a detailed output of the captured packet information. |
| **parameter** | Reconstructs and displays EXEC commands that were used to specify the capture. |
| **detailed** | Provides a detailed output of the captured packet information. |

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.12.1 | This command was introduced. |

## Usage Guidelines

You can enter the **show monitor capture** command when the capture buffer is not in the running state.

If you enter the **detail** keyword, packets are decoded to the Layer 4 protocol level and displayed. If you enter the **dump** keyword, non-IP packets are displayed in hexadecimal dump format. An ACL can be configured as a display filter so that only packets permitted by the ACL are displayed.

The following example shows how to display all the packets in a capture buffer. The output is self-explanatory.

```
Device# show monitor capture mycap buffer

buffer size (KB) : 2048000
buffer used (KB) : 128
packets in buf : 17
packets dropped : 0
packets per sec : 3
```

The following example shows how to display the list of commands that were used to specify the capture:

```
Device# show monitor capture cap1 parameter

  monitor capture cap1 interface GigabitEthernet 1/0/1 both
  monitor capture cap1 match any
  monitor capture cap1 buffer size 10
  monitor capture cap1 limit pps 1000
```

The following example shows how to display brief output from the captured packet information. The output is self-explanatory.

```
Device# show monitor capture cap1 buffer brief

------------------------------------------------------------------
#   size   timestamp     source            destination   protocol
------------------------------------------------------------------
   0   62    0.000000   10.0.0.1         ->  203.0.113.254  UDP
   1   46    0.267992   10.0.1.2         ->  203.0.113.204  IGMP
   2   76    0.428979   172.16.255.3     ->  172.16.255.3   UDP
   3   62    1.613982   10.0.29.1        ->  172.16.200.2   UDP
   4   74    1.659970   10.0.1.3         ->  10.0.0.10      EIGRP
   5   90    2.016006   10.29.0.4        ->  203.0.113.224  UDP
   6   74    2.088008   10.1.9.2         ->  203.0.113.10   EIGRP
   7   76    2.114008   172.17.254.1     ->  172.16.255.1   UDP
   8   74    2.245990   10.29.0.3        ->  203.0.113.10   EIGRP
   9   46    2.262987   10.0.0.0         ->  203.0.113.1    IGMP
  10   77    2.362988   10.1.9.2         ->  203.0.113.10   EIGRP
  11   62    2.631971   10.29.0.2        ->  203.0.113.2    UDP
  12   74    2.934009   10.29.0.5        ->  203.0.113.10   EIGRP
  13   74    3.331984   10.29.0.6        ->  203.0.113.10   EIGRP
  14   46    3.499974   10.0.0.0         ->  203.0.113.1    IGMP
  15   46    4.304992   10.0.0.0         ->  203.0.113.1    IGMP
  16   76    5.157005   172.16.255.3     ->  172.17.255.3   UDP
```

The following example shows how to display all the packets in a capture buffer. The output is self-explanatory.

```
Device# show monitor capture cap1 buffer detailed

 -----------------------------------------------------------------
#   size   timestamp     source            destination   protocol
------------------------------------------------------------------
   0   62    0.000000   10.29.0.2         ->  172.16.255.3   UDP
  0000:  01005E00 00020000 0C07AC1D 080045C0   ..^...........E.
  0010:  00300000 00000111 CFDC091D 0002E000   .0..............
  0020:  000207C1 07C1001C 802A0000 10030AFA   .........*......
  0030:  1D006369 73636F00 0000091D 0001       ..example.......

   1   46    0.267992   10.0.0.0          ->  172.16.255.1   IGMP
  0000:  01005E00 0002001B 2BF69280 080046C0   ..^.....+.....F.
  0010:  00200000 00000102 44170000 0000E000   . ......D.......
  0020:  00019404 00001700 E8FF0000 0000       ..............

   2   76    0.428979   172.16.255.3     ->  172.17.255.3    UDP
  0000:  00000C07 AC1DB414 89031124 080045C0   ...........$..E.
  0010:  003E0000 0000FF11 64C5AC10 FF03AC11   .>......d.......
  0020:  FF030286 0286002A 84A40001 001EAC10   .......*........
  0030:  FF030000 01000014 00000000 04000004   ................

   3   62    1.613982   10.26.11.3        ->  172.16.255.1    UDP
  0000:  01005E00 0002001B 2BF68680 080045C0   ..^.....+.....E.
  0010:  00300000 00000111 CFDB091D 0003E000   .0..............
  0020:  000207C1 07C1001C 88B50000 08030A6E   ...............n
  0030:  1D006369 73636F00 0000091D 0001       ..example.......

   4   74    1.659970   10.29.3.2         ->  172.16.255.2   EIGRP
  0000:  01005E00 000A001B 2BF69280 080045C0   ..^.....+.....E.
  0010:  003C0000 00000258 CE81091D 0002E000   .<.....X........
  0020:  000A0205 F3000000 00000000 00000000   ................
  0030:  00000000 00D10001 000C0100 01000000   ................

   5   90    2.016006   10.22.1.4         ->  203.0.113.1     UDP
  0000:  FFFFFFFF FFFF001C 0F2EDC00 080045C0   ..............E.
  0010:  004C0000 00000111 AFC1091D 0004FFFF   .L..............
  0020:  FFFF007B 007B0038 5B14E500 06E80000   ...{.{.8[.......
  0030:  00000021 BE23494E 49540000 00000000   ...!.#INIT......
```

The following example shows how to display a hexadecimal dump of the captured packet:

```
Device# show monitor capture cap1 buffer dump
0
 0000:  01005E00 00020000 0C07AC1D 080045C0   ..^...........E.
 0010:  00300000 00000111 CFDC091D 0002E000   .0..............
 0020:  000207C1 07C1001C 802A0000 10030AFA   .........*......
 0030:  1D006369 73636F00 0000091D 0001       ..example.......

1
 0000:  01005E00 0002001B 2BF69280 080046C0   ..^.....+.....F.
 0010:  00200000 00000102 44170000 0000E000   . ......D.......
 0020:  00019404 00001700 E8FF0000 0000       ..............

2
 0000:  01005E00 0002001B 2BF68680 080045C0   ..^.....+.....E.
 0010:  00300000 00000111 CFDB091D 0003E000   .0..............
 0020:  000207C1 07C1001C 88B50000 08030A6E   ...............n
 0030:  1D006369 73636F00 0000091D 0001       ..example.......

3
 0000:  01005E00 000A001C 0F2EDC00 080045C0   ..^...........E.
 0010:  003C0000 00000258 CE7F091D 0004E000   .<.....X........
 0020:  000A0205 F3000000 00000000 00000000   ................
 0030:  00000000 00D10001 000C0100 01000000   ................
 0040:  000F0004 00080501 0300               ..........
```

# show 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 Gibraltar 16.10.1 | 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

This example shows how to see NMSP cloud-service statistics:

```
Device# show nmsp cloud-services statistics
```

# show 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

This example shows how to see NMSP cloud-service summary information:

```
Device# show nmsp cloud-services summary
```

# show nmsp subscription group detail all

To display the mobility services group subscription details of all CMX connections, use the **show nmsp subscription group detail all** command.

**show nmsp subscription group detail all**

### Syntax Description

This command has no keywords or arguments.

### Command Default

None

### Command Modes

Privileged EXEC (#)

### Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

### Example

The following example shows how to display the mobility services group subscription details of all CMX connections:

```
Device# show nmsp subscription group detail all
```

# show nmsp subscription group detail ap-list

To display the AP MAC list subscribed for a group by a CMX connection, use the **show nmsp subscription group detail ap-list** command.

**show nmsp subscription group detail ap-list** *group-name cmx-IP-addrress*

## Syntax Description

| | |
|---|---|
| *group-name* | CMX AP group name. |
| *cmx-IP-addrress* | CMX IP address. |

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

### Example

The following example shows how to verify the AP MAC list subscribed for a group by a CMX connection.

```
Device# show nmsp subscription group detail ap-list Group1 127.0.0.1

CMX IP address: 127.0.0.1
CMX Group name: Group1
CMX Group AP MACs:
: 00:00:00:00:70:02  00:00:00:00:66:02  00:99:00:00:00:02  00:00:00:bb:00:02
  00:00:00:00:55:02  00:00:00:00:50:02  00:33:00:00:00:02  00:d0:00:00:00:02
  00:10:00:10:00:02  00:00:00:06:00:02  00:00:00:02:00:02  00:00:00:00:40:02
  00:00:00:99:00:02  00:00:00:00:a0:02  00:00:77:00:00:02  00:22:00:00:00:02
  00:00:00:00:00:92  00:00:00:00:00:82  00:00:00:00:03:02  aa:00:00:00:00:02
  00:00:00:50:00:42  00:00:0d:00:00:02  00:00:00:00:00:32  00:00:00:cc:00:02
  00:00:00:88:00:02  20:00:00:00:00:02  10:00:00:00:00:02  01:00:00:00:00:02
  00:00:00:00:00:02  00:00:00:00:00:01  00:00:00:00:00:00
```

# show nmsp subscription group detail services

To display the services subscribed for a group by a CMX connection, use the **show nmsp subscription group detail services** command.

**show nmsp subscription group detail services** *group-name cmx-IP-addrress*

## Syntax Description

| | |
|---|---|
| *group-name* | CMX AP group name. |
| *cmx-IP-addrress* | CMX IP address. |

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

### Example

The following example shows how to verify the services subscribed for a group by a CMX connection.

```
Device# show nmsp subscription group detail services Group1 127.0.0.1

CMX IP address: 127.0.0.1
CMX Group name: Group1
CMX Group filtered services:
Service            Subservice
-----------------------------
RSSI               Mobile Station,
Spectrum
Info
Statistics
```

# show nmsp subscription group summary

To display the mobility services group subscription summary of all CMX connections, use the **show nmsp subscription group summary** command.

**show nmsp subscription group summary**

## Syntax Description

This command has no keywords or arguments.

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

### Example

The following example shows how to verify the mobility services group subscription summary of all CMX connections.

```
Device# show nmsp subscription group summary

CMX IP address: 127.0.0.1
  Groups subscribed by this CMX server:
  Group name: Group1
```

# show ntp associations

To display the status of Network Time Protocol (NTP) associations, use the **show ntp associations** command in privileged EXEC mode.

**show ntp associations**

## Syntax Description

This command has no keywords or arguments.

## Command Default

None

## Command Modes

Privileged EXEC(#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Example

The following example shows how to view NTP associations. :

```
Device# show ntp associations
  address         ref clock       st   when   poll reach  delay  offset   disp
*~10.1.1.99       72.163.32.44     2    918   1024   377  0.177   7.618  1.102
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
--
```

# show parameter-map type webauth name

To verify the webauth parameters of a parameter map, use the **show parameter-map type webauth name** command.

**show parameter-map type webauth name** *parameter-map name*

## Syntax Description

| | |
|---|---|
| *parameter-map name* | Name of the parameter map. |

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

## Examples

The following example shows how to verify the webauth parameters of a parameter map:

```
Device# configure terminal
Device(config)# show parameter-map type webauth name parameter-map-name
```

# show platform conditions

To see information about conditional debugs, use the **show platform conditions** command.

**show platform conditions**

### Command Default

None

### Command Modes

Privileged EXEC

### Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see information about conditional debugs:

```
Device# show platform conditions
```

# show platform hardware

To see the hardware platform Quantum flow processor datapath statistics, use the **show platform hardware chassis active qfp feature wireless wlclient datapath cpp-if-handle statistics** command.

**show hardware chassis active qfp feature wireless wlclient datapath cpp-if-handle** *client-cpp-value* **statistics** {**clear** | **start** | **stop**}

## Syntax Description

| | |
|---|---|
| **active** | Active instance. |
| **qfp** | Quantum Flow Processor. |
| **wlclient** | QFP wireless client. |
| **cpp-if-handle** | client cpp interface handle. |
| *client-cpp-value* | Client cpp if-handle value. The range is between 1 and 4294967295. |
| **statistics** | Show Client Statistics. |
| **clear** | Shows and Clears the Client Statistics. |
| **start** | Start Client Statistics collection. |
| **stop** | Stop Client Statistics collection. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to start client statistics collection:

```
Device# show platform hardware chassis active qfp feature wireless wlclient datapath
cpp-if-handle cpp-if-handle value statistics start
```

# show platform hardware chassis active qfp feature dns-snoop-agent client enabled-intf

To view the DSA enabled interfaces, use the **show platform hardware chassis active qfp feature dns-snoop-agent client enabled-intf** command.

**show platform hardware chassis active qfp feature dns-snoop-agent client enabled-intf**

## Syntax Description

This command has no arguments.

## Command Default

None

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the DSA enabled interfaces:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent client enabled-intf
Interface name: GigabitEthernet0/0/0, handle: 5
```

# show platform hardware chassis active qfp feature dns-snoop-agent client hw-pattern-list

To view the OpenDNS string or FQDN filter for the pattern list, use the **show platform hardware chassis active qfp feature dns-snoop-agent client hw-pattern-list** command.

**show platform hardware chassis active qfp feature dns-snoop-agent client hw-pattern-list** {**fqdn-filter** *fqdn_filter_ID* | **odns_string**}

## Syntax Description

| | |
|---|---|
| **fqdn-filter** | Displays the FQDN filter for the pattern list. |
| *fqdn_filter_ID* | Refers to the FQDN filter ID. The valid range is from 1 to 16. |
| **odns_string** | Displays the OpenDNS string for the pattern list. |

## Command Default

None

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the FQDN filter for the pattern list:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent client
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.

**show platform hardware chassis active qfp feature dns-snoop-agent client info**

## Syntax Description

This command has no arguments.

## Command Default

None

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the DSA client details:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent client info
Number of patterns added/deleted/total: 2/0/2
Number of re_table rebuilt : : 0
Number of str_table rebuilt: : 2
Registered clients: 0x001ffff0
Number of transaction started/ended: 2/2
Memory pool size/limit: 512/81920
Pending Deletion Pattern List:
```

# show platform hardware chassis active qfp feature dns-snoop-agent client pattern-list

To view the OpenDNS string or FQDN filter for the pattern list, use the **show platform hardware chassis active qfp feature dns-snoop-agent client pattern-list** command.

**show platform hardware chassis active qfp feature dns-snoop-agent client pattern-list** {**fqdn-filter** *fqdn_filter_ID* | **odns_string**}

### Syntax Description

| | |
|---|---|
| **fqdn-filter** | Displays the FQDN filter for the pattern list. |
| *fqdn_filter_ID* | Refers to the FQDN filter ID. The valid range is from 1 to 16. |
| **odns_string** | Displays the OpenDNS string for the pattern list. |

### Command Default

None

### Command Modes

Global configuration

### Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the FQDN filter for the pattern list:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent client pattern-list
 fqdn-filter 1
Filter Name: urllist_flex_preauth
Pattern List in CPP client: 1

Name: url1.dns.com
feature_mask: 0x00000010, hw_ptr: 0xdf86d510
```

# show platform hardware chassis active qfp feature dns-snoop-agent datapath ip-cache

To view the DSA IP cache table details, use the **show platform hardware chassis active qfp feature dns-snoop-agent datapath ip-cache** command.

**show platform hardware chassis active qfp feature dns-snoop-agent datapath ip-cache** {**address** [**ipv4** *ipv4_address* | **ipv6** *ipv6_address*] | **all** | **pattern** *regex_pattern*}

## Syntax Description

| | |
|---|---|
| **address** [**ipv4** *ipv4_address* \| **ipv6** *ipv6_address*] | Displays the DSA address entry details |
| **all** | Displays all the DSA IP cache address details |
| **pattern** *regex_pattern* | Displays the DSA IP cache pattern details |

## Command Default

None

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the DSA address entry details:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent datapath ip-cache
 address ipv4 104.122.2.194
IP address: 104.122.2.194, client(s): 32, regex: www.adobe.com, expire in 0 seconds
```

This example shows how to view all the DSA IP cache address details:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent datapath ip-cache
 all
IP Address        Client(s) Expire     Match         RegexId      Dirty
------------------------------------------------------------------------
172.217.13.228      2       132     .*google.com    0x4d7f9e20     0x0
```

This example shows how to view the DSA IP cache pattern details:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent datapath ip-cache
 pattern .*google*
1 IP Addresses matching pattern .*google*
IP Address                    Client(s)  Expire   Match       RegexId    Dirty
-------------------------------------------------------------------------------
2607:f8b0:4004:800:0:0:0:2004   32         13    .*google*   0x31156220   0x0
```

# show platform hardware chassis active qfp feature dns-snoop-agent datapath memory

To view the DSA datapath memory details, use the **show platform hardware chassis active qfp feature dns-snoop-agent datapath memory** command.

**show platform hardware chassis active qfp feature dns-snoop-agent datapath memory**

## Syntax Description

This command has no arguments.

## Command Default

None

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the DSA datapath memory details:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent datapath memory
Table-Name   Address      Size
-----------------------------------------
IP Cache DB   0xda5bb420   512
IP Hash       0xda41f400   1024
String Table  0xdec6ac10
String Table  0xda41f010

==DSA Chunk info==
Chunk-Pool   Allocated     Total_Free   Init-Num     Low_Wat
------------------------------------------------------------
ip cache chunk   0            512          512          512

==DSA Runtime Info==
------------------------------------------------------------
dsa init state 0x7   dsa client mask 0x100010
```

# show platform hardware chassis active qfp feature dns-snoop-agent datapath regexp-table

To view the DSA regular expression table, use the **show platform hardware chassis active qfp feature dns-snoop-agent datapath regexp-table** command.

**show platform hardware chassis active qfp feature dns-snoop-agent datapath regexp-table**

## Syntax Description

This command has no arguments.

## Command Default

None

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the DSA regular expression table:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent datapath
regexp-table
String Table 0xdec6ac10     WLS_FQDN_GRP_1
String Table 0xda41f010     ODNS String
```

# show platform hardware chassis active qfp feature dns-snoop-agent datapath stats

To view the DSA statistics, use the **show platform hardware chassis active qfp feature dns-snoop-agent datapath stats** command.

**show platform hardware chassis active qfp feature dns-snoop-agent datapath stats**

### Syntax Description

This command has no arguments.

### Command Default

None

### Command Modes

Global configuration

### Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the DSA statistics:

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent datapath stats
DNS Snoop Agent Stats:
  parser unknown pkt: 0
  parser not needed: 0
  parser fmt error: 0
  parser pa error: 0
  parser non resp: 0
  parser multiple name: 0
  parser dns name err: 0
  parser matched ip: 0
  parser redirect: 0
  parser whitelist redirect: 0
  parser blacklist redirect: 0
  parser invalid redirect ip: 0
  parser skip: 0
  regex locked: 0
  regex not matched: 0
  pkt drop whitelist no redirect ip: 0
  pkt drop blacklist no redirect ip: 0
  entries in use: 0
  ip cache allocation fail: 0
  ip addr add: 0
  ip addr update: 0
  ip addr delete: 0
  ip addr cache hit: 0
  ip addr cache miss: 0
  ip addr bad param: 0
  ip addr delete not found: 0
  ip cache not initialized: 0
```

# show platform hardware chassis active qfp feature et-analytics datapath runtime

To view the ETA global state in datapath, use the **show platform hardware chassis active qfp feature et-analytics datapath runtime** command.

**show platform hardware chassis active qfp feature et-analytics datapath runtime**

## Syntax Description

This command has no keywords or arguments.

## Command Default

None

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.11.1 | This command was introduced. |

This example shows how to view the ETA global and interface details:

```
Device# show platform hardware chassis active qfp feature et-analytics datapath runtime
ET-Analytics run-time information:
   Feature state: initialized (0x00000004)
   Inactive timeout : 15 secs (default 15 secs)
   WhiteList information :
      flag: False
      cgacl w0 : n/a
      cgacl w1 : n/a
   Flow CFG information :
      instance ID : 0x0
      feature ID : 0x1
      feature object ID : 0x1
      chunk ID : 0xC
```

# show platform hardware chassis active qfp feature et-analytics datapath memory

To view the ETA memory details, use the **show platform hardware chassis active qfp feature et-analytics datapath memory** command.

**show platform hardware chassis active qfp feature et-analytics datapath memory**

### Syntax Description

This command has no arguments.

### Command Default

None

### Command Modes

Global configuration

### Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the ETA memory details:

```
Device# show platform hardware chassis active qfp feature et-analytics datapath memory
ET-Analytics memory information:
   Size of FO : 3200 bytes
   No. of FO allocs : 0
   No. of FO frees : 0
```

# show platform hardware chassis active qfp feature et-analytics datapath stats export

To view the ETA flow export in datapath, use the **show platform hardware chassis active qfp feature et-analytics datapath stats export** command.

**show platform hardware chassis active qfp feature et-analytics datapath stats export**

**Syntax Description**

This command has no arguments.

**Command Default**

None

**Command Modes**

Global configuration

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the ETA flow export in datapath:

```
Device# show platform hardware chassis active qfp feature et-analytics datapath stats export
ET-Analytics 192.168.5.2:2055 vrf 0 Stats:
   Export statistics:
      Total records exported : 5179231
      Total packets exported : 3124873
      Total bytes exported : 3783900196
      Total dropped records : 0
      Total dropped packets : 0
      Total dropped bytes : 0
      Total IDP records exported :
            initiator->responder : 1285146
            responder->initiator : 979284
      Total SPLT records exported:
            initiator->responder : 1285146
            responder->initiator : 979284
      Total SALT records exported:
            initiator->responder : 0
            responder->initiator : 0
      Total BD records exported :
            initiator->responder : 0
            responder->initiator : 0
      Total TLS records exported :
            initiator->responder : 309937
            responder->initiator : 329469
```

# show platform hardware chassis active qfp feature et-analytics datapath stats flow

To view the ETA flow statistics, use the **show platform hardware chassis active qfp feature et-analytics datapath stats flow** command.

**show platform hardware chassis active qfp feature et-analytics datapath stats flow**

## Syntax Description

This command has no arguments.

## Command Default

None

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the ETA flow statistics:

```
Device# show platform hardware chassis active qfp feature et-analytics datapath stats flow
ET-Analytics Stats:
   Flow statistics:
      feature object allocs : 0
      feature object frees : 0
      flow create requests : 0
      flow create matching : 0
      flow create successful: 0
      flow create failed, CFT handle: 0
      flow create failed, getting FO: 0
      flow create failed, malloc FO : 0
      flow create failed, attach FO : 0
      flow create failed, match flow: 0
      flow create, aging already set: 0
      flow ageout requests : 0
      flow ageout failed, freeing FO: 0
      flow ipv4 ageout requests : 0
      flow ipv6 ageout requests : 0
      flow whitelist traffic match : 0
```

# show platform hardware chassis active qfp feature wireless et-analytics eta-pending-client-tree

To view clients in the ETA pending wireless client tree, use the **show platform hardware chassis active qfp feature wireless et-analytics eta-pending-client-tree** command.

**show platform hardware chassis active qfp feature wireless et-analytics eta-pending-client-tree**

## Syntax Description

This command has no arguments.

## Command Default

None

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view clients in the ETA pending wireless client tree:

```
Device# show platform hardware chassis active qfp feature wireless et-analytics
eta-pending-client-tree
CPP IF_H    DPIDX        MAC Address     VLAN   AS  MS  WLAN        POA
---------------------------------------------------------------------------
0X2A      0XA0000001    2c33.7a5b.827b   160    RN  LC ewlc_ssid 0x90000003
0X2B      0XA0000002    2c33.7a5b.80fb   160    RN  LC ewlc_ssid 0x90000003
```

# show platform hardware chassis active qfp feature wireless et-analytics statistics

To view the ETA pending wireless client tree statistics, use the **show platform hardware chassis active qfp feature wireless et-analytics statistics** command.

**show platform hardware chassis active qfp feature wireless et-analytics statistics**

### Syntax Description

This command has no arguments.

### Command Default

None

### Command Modes

Global configuration

### Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the ETA pending wireless client tree statistics:

```
Device# show platform hardware chassis active qfp feature wireless et-analytics statistics
Wireless ETA cpp-client plumbing statistics
Number of ETA pending clients : 2
Counter                                             Value
-------------------------------------------------------------------
Enable ETA on wireless client called                  0
Delete ETA on wireless client called                  0
ETA global cfg init cb TVI FIA enable error           0
ETA global cfg init cb output SB read error           0
ETA global cfg init cb output SB write error          0
ETA global cfg init cb input SB read error            0
ETA global cfg init cb input SB write error           0
ETA global cfg init cb TVI FIA enable success         0
ETA global cfg uninit cb ingress feat disable         0
ETA global cfg uninit cb ingress cfg delete           0
ETA global cfg uninit cb egress feat disable          0
ETA global cfg uninit cb egress cfg delete er         0
ETA pending list insert entry called                  4
ETA pending list insert invalid arg error             0
ETA pending list insert entry exists error            0
ETA pending list insert no memory error               0
ETA pending list insert entry failed                  0
ETA pending list insert entry success                 4
ETA pending list delete entry called                  2
ETA pending list delete invalid arg error             0
ETA pending list delete entry missing                 0
ETA pending list delete entry remove error            0
ETA pending list delete entry success                 2
```

# show platform hardware slot R0 ha_port interface stats

To see the HA port interface setting status, use the **show platform hardware slot R0 ha_port interface stats** command.

**show platform hardware slot R0 ha_port interface stats**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Bengaluru 17.5.1 | This command was introduced. |

## Examples

This example shows how to see the HA port interface setting status:

```
Device# show platform hardware slot R0 ha_port interface stats
HA Port
ha_port   Link encap:Ethernet  HWaddr 70:18:a7:c8:80:70
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
          Memory:e0900000-e0920000


Settings for ha_port:
        Supported ports:            [ TP ]
        Supported link modes:       10baseT/Half 10baseT/Full
                                    100baseT/Half 100baseT/Full
                                    1000baseT/Full
        Supported pause frame use:   Symmetric
        Supports auto-negotiation:   Yes
        Supported FEC modes:         Not reported
        Advertised link modes:       10baseT/Half 10baseT/Full
                                     100baseT/Half 100baseT/Full
                                     1000baseT/Full
        Advertised pause frame use:  Symmetric
        Advertised auto-negotiation: Yes
        Advertised FEC modes:        Not reported
        Speed:                       Unknown!
        Duplex:                      Unknown! (255)
        Port:                        Twisted Pair
        PHYAD:                       1
        Transceiver:                 internal
        Auto-negotiation:            on
        MDI-X:                       off (auto)
        Supports Wake-on:            pumbg
        Wake-on:                     g
        Current message level:       0x00000007 (7)
                                     drv probe link
        Link detected:               no
```

```
NIC statistics:
     rx_packets:             0
     tx_packets:             0
     rx_bytes:               0
     tx_bytes:               0
     rx_broadcast:           0
     tx_broadcast:           0
     rx_multicast:           0
     tx_multicast:           0
     multicast:              0
     collisions:             0
     rx_crc_errors:          0
     rx_no_buffer_count:     0
     rx_missed_errors:       0
     tx_aborted_errors:      0
     tx_carrier_errors:      0
     tx_window_errors:       0
     tx_abort_late_coll:     0
     tx_deferred_ok:         0
     tx_single_coll_ok:      0
     tx_multi_coll_ok:       0
     tx_timeout_count:       0
     rx_long_length_errors:  0
     rx_short_length_errors: 0
     rx_align_errors:        0
     tx_tcp_seg_good:        0
     tx_tcp_seg_failed:      0
     rx_flow_control_xon:    0
     rx_flow_control_xoff:   0
     tx_flow_control_xon:    0
     tx_flow_control_xoff:   0
     rx_long_byte_count:     0
     tx_dma_out_of_sync:     0
     tx_smbus:               0
     rx_smbus:               0
     dropped_smbus:          0
     os2bmc_rx_by_bmc:       0
     os2bmc_tx_by_bmc:       0
     os2bmc_tx_by_host:      0
     os2bmc_rx_by_host:      0
     tx_hwtstamp_timeouts:   0
     rx_hwtstamp_cleared:    0
     rx_errors:              0
     tx_errors:              0
     tx_dropped:             0
     rx_length_errors:       0
     rx_over_errors:         0
     rx_frame_errors:        0
     rx_fifo_errors:         0
     tx_fifo_errors:         0
     tx_heartbeat_errors:    0
     tx_queue_0_packets:     0
     tx_queue_0_bytes:       0
     tx_queue_0_restart:     0
     tx_queue_1_packets:     0
     tx_queue_1_bytes:       0
     tx_queue_1_restart:     0
     rx_queue_0_packets:     0
     rx_queue_0_bytes:       0
     rx_queue_0_drops:       0
     rx_queue_0_csum_err:    0
     rx_queue_0_alloc_failed:0
     rx_queue_1_packets:     0
```

```
rx_queue_1_bytes:       0
rx_queue_1_drops:       0
rx_queue_1_csum_err:    0
rx_queue_1_alloc_failed:0
```

# show platform software system all

To check status of the current virtual machine and look for performance issues due to inadequate resources (or other issues with the hosting environment), use the **set platform software system all** command in privileged EXEC mode.

**show platform software system all**

## Syntax Description

This command has no keywords or arguments.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Examples

This example shows how to check status of the current virtual machine and its resources:

```
Device# show platform software system all

Processor Details
=================
Number of Processors : 6
Processor : 1 - 6
vendor_id : GenuineIntel
cpu MHz  : 2593.750
cache size : 35840 KB
Crypto Supported : Yes
model name : Intel(R) Xeon(R) CPU E5-2690 v4 @ 2.60GHz

Memory Details
==============
Physical Memory : 16363904KB

VNIC Details
============
Name   Mac Address  Status Platform MTU
GigabitEthernet1 000c.2964.7126  UP 1500
GigabitEthernet2 000c.2964.7130  UP 1500

Hypervisor Details
===================
Hypervisor: VMWARE
Manufacturer: VMware, Inc.
Product Name: VMware Virtual Platform
Serial Number: VMware-56 4d e5 0a a7 dd 27 2b-0e 2f 36 6e 0f 64 71 26
UUID: 564DE50A-A7DD-272B-0E2F-366E0F647126
image_variant :

Boot Details
===================
Boot mode: BIOS
Bootloader version: 1.1
```

# show platform software trace filter-binary

To display the most recent trace information for a specific module, use the **show platform software trace filter-binary** command in privileged EXEC or user EXEC mode.

**show platform software trace filter-binary***modules* [**context** *mac-address*]

## Syntax Description

| | |
|---|---|
| **context***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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

This command collates and sorts all the logs present in the `/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

| | |
|---|---|
| **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

| Release | Modification |
|---|---|
| | This command was introduced. |

## 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 wireless** [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

## Syntax Description

| | |
|---|---|
| *process* | Process whose tracing level is being set. Options include:<br>• **chassis-manager**—The Chassis Manager process.<br>• **cli-agent**—The CLI Agent process.<br>• **cmm**—The CMM process.<br>• **dbm**—The Database Manager process.<br>• **emd**—The Environmental Monitoring process.<br>• **fed**—The Forwarding Engine Driver process.<br>• **forwarding-manager**—The Forwarding Manager process.<br>• **geo**—The Geo Manager process.<br>• **host-manager**—The Host Manager process.<br>• **interface-manager**—The Interface Manager process.<br>• **iomd**—The Input/Output Module daemon (IOMd) process.<br>• **ios**—The IOS process.<br>• **license-manager**—The License Manager process.<br>• **logger**—The Logging Manager process.<br>• **platform-mgr**—The Platform Manager process.<br>• **pluggable-services**—The Pluggable Services process.<br>• **replication-mgr**—The Replication Manager process.<br>• **shell-manager**—The Shell Manager process.<br>• **sif**—The Stack Interface (SIF) Manager process.<br>• **smd**—The Session Manager process.<br>• **stack-mgr**—The Stack Manager process.<br>• **table-manager**—The Table Manager Server.<br>• **thread-test**—The Multithread Manager process.<br>• **virt-manager**—The Virtualization Manager process.<br>• **wireless**—The wireless controller module process. |

| | |
|---|---|
| *slot* | Hardware slot where the process for which the trace level is set, is running. Options include:<br>• *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.<br>• *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.<br>• **F0**—The Embedded Service Processor in slot 0.<br>• **F1**—The Embedded Service Processor in slot 1.<br>• **FP active**—The active Embedded Service Processor.<br>• **R0**—The route processor in slot 0.<br>• **RP active**—The active route processor.<br>• **switch** <*number*> —The switch, with its number specified.<br>• **switch active**—The active switch.<br>• **switch standby**—The standby switch.<br>  • *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.<br>  • *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.<br>  • **F0**—The Embedded Service Processor in slot 0.<br>  • **FP active**—The active Embedded Service Processor.<br>  • **R0**—The route processor in slot 0.<br>  • **RP active**—The active route processor. |

## 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 Modes

User EXEC (>)

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Examples

This example shows how to view the trace level:

```
Device# show platform software trace level dbm switch active R0
Module Name                      Trace Level
-------------------------------------------------
binos                            Notice
binos/brand                      Notice
bipc                             Notice
btrace                           Notice
bump_ptr_alloc                   Notice
cdllib                           Notice
chasfs                           Notice
dbal                             Informational
dbm                              Debug
evlib                            Notice
evutil                           Notice
file_alloc                       Notice
green-be                         Notice
ios-avl                          Notice
klib                             Debug
services                         Notice
sw_wdog                          Notice
syshw                            Notice
tdl_cdlcore_message              Notice
tdl_dbal_root_message            Notice
tdl_dbal_root_type               Notice
```

# show platform software 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*

## Command Modes

User EXEC (>)

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Examples

This example shows how to 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]
10/30 09:42:48.762 [btrace] [8974]: (note): Successfully registered module [98]
[tdl_cdlcore_message]
10/29 13:28:19.023 [stack_mgr] [8974]: (note): Examining peer state
10/29 13:28:19.023 [stack_mgr] [8974]: (note): no switch eligible for standby election
presently
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 13:26:46.584 [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 chassis active R0

To display the trace message for license-manager process of active route processor, use the **show platform software trace message license-manager chassis active R0** command in privileged EXEC mode.

`show platform software trace message license-managerchassis` {*chassis-number* `| active | standby`}`R0reverse`

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

### Example

This example shows how to display the trace messages for the Forwarding Engine Driver processes:

```
Device# show platform software trace message license-manager chassis active R0
.......
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(50:50:0:7)
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}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
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 07:54:30.547 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:30.537 {lman_R0-0}{1}: [bipc] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Pending connection to server 10.0.1.0
2018/06/20 07:54:29.546 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:28.545 {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):
Flag tdlh stale epoch for all tdl handles
2018/06/20 07:54:20.536 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Chasfs 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
/tmp/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/
2018/06/20 07:54:20.536 {lman_R0-0}{1}: [bcrdu] [21231]: UUID: 0, ra: 0, TID: 0 (note):
CRDU
/tmp/sw/mount/isr4400v2-mono-universalk9.BLD_V169_THROTTLE_LATEST_20180618_044856_V16_9_0_163.SSA.pkg/usr/binos/bin/lman
 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.

**show platform software trace message license-manager** [ **chassis** { *chassis-number* | **active** | **standby** } **R0** ]

## Syntax Description

| | |
|---|---|
| **active R0** | Active instance in Route-processor slot 0. |
| **standby R0** | Standby instance in Route-processor slot 0. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.12.2s | This command was introduced. |

### Example

This example shows how to display the trace messages for the Forwarding Engine Driver processes:

```
Device# show platform software trace message license-manager chassis active 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_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}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
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 07:54:30.547 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:30.537 {lman_R0-0}{1}: [bipc] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Pending connection to server 10.0.1.0
2018/06/20 07:54:29.546 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR): The
ipc information for IOS is invalid
2018/06/20 07:54:28.545 {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):
Flag tdlh stale epoch for all tdl handles
2018/06/20 07:54:20.536 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Chasfs 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
/tmp/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/
2018/06/20 07:54:20.536 {lman_R0-0}{1}: [bcrdu] [21231]: UUID: 0, ra: 0, TID: 0 (note):
CRDU
/tmp/sw/mount/isr4400v2-mono-universalk9.BLD_V169_THROTTLE_LATEST_20180618_044856_V16_9_0_163.SSA.pkg/usr/binos/bin/lman
```

```
 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
```

# show platform software utd chassis active F0 et-analytics global

To view the ETA global and interface details, use the **show platform software utd chassis active F0 et-analytics global** command.

**show platform software utd chassis active F0 et-analytics global**

## Syntax Description

This command has no arguments.

## Command Default

None

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the ETA global and interface details:

```
Device# show platform software utd chassis active F0 et-analytics global
ET Analytics Global Configuration
ID: 1
All Interfaces: Off
IP address and port and vrf: 192.168.5.2:2055:0
```

# show platform software et-analytics global

To view the ETA global configuration, use the **show platform software et-analytics global** command.

**Note** The **show platform software et-analytics global** command does not display the ETA enabled wireless client interfaces.

**show platform software et-analytics global**

## Syntax Description

This command has no arguments.

## Command Default

None

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the ETA global and interface details:

```
Device# show platform software et-analytics global
ET-Analytics Global state
=========================
All Interfaces : Off
IP Flow-record Destination: 192.168.5.2 : 2055
Inactive timer: 15
```

# show 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the Umbrella global parameter map details:

```
Device# show parameter-map type umbrella global
parameter-map type umbrella global
   token   57CC80106C087FB1B2A7BAB4F2F4373C00247166
   local-domain dns_wl
   dnscrypt
   udp-timeout 2
   resolver ipv4 208.67.220.220
   resolver ipv4 208.67.222.222
   resolver ipv6 2620:119:53::53
   resolver ipv6 2620:119:35::35
```

# show policy-map

To display quality of service (QoS) policy maps, which define classification criteria for incoming traffic, use the **show policy-map** command in EXEC mode.

**show policy-map** [*policy-map-name* | **interface** *interface-id*]

**show policy-map interface** {**Auto-template** | **Capwap** | **GigabitEthernet** | **GroupVI** | **InternalInterface** | **Loopback** | **Lspvif** | **Null** | **Port-channel** | **TenGigabitEthernet** | **Tunnel** | **Vlan** | **brief** | **class** | **input** | **output**

**show policy-map interface** {**ap name** *ap_name* | **client mac** *mac_address* | **radio type** {**24ghz** | **5ghz**} **ap name** *ap_name* | **ssid name** *ssid_name* {**ap name** *ap_name* | **radio type** {**24ghz** | **5ghz**} **ap name** *ap_name*} }

## Syntax Description

| | |
|---|---|
| *policy-map-name* | (Optional) Name of the policy-map. |
| **interface** *interface-id* | (Optional) Displays the statistics and the configurations of the input and output policies that are attached to the interface. |
| **ap name** *ap_name* | Displays SSID policy configuration of an access point. |
| **client mac** *mac_address* | Displays information about the policies for all the client targets. |
| **radio type** {**24ghz** \| **5ghz** | Displays policy configuration of the access point in the specified radio type. |
| **ssid name** *ssid_name* | Displays policy configuration of an SSID. |

## Command Modes

User EXEC

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This comman |

## Usage Guidelines

Policy maps can include policers that specify the bandwidth limitations and the action to take if the limits are exceeded.

**Note**

Though visible in the command-line help string, the **control-plane**, **session**, and **type** keywords are not supported, and the statistics shown in the display should be ignored.

To display classification counters for ternary content addressable memory (TCAM) (marking or policing) based policies, enter the interface ID. Classification counters have the following restrictions:

- Classification counters are supported only on wired ports (in the ingress and egress directions).
- Classification counters count packets instead of bytes.
- Only QoS configurations with marking or policing trigger the classification counter.
- As long as there is policing or marking action in the policy, the class-default will have classification counters.
- Classification counters are not port based. The counters are shared across targets sharing the same policy map. This means that the classification counter aggregates all packets belonging to the same class of the same policy which attach to different interfaces.

This is an example of output from the **show policy-map interface** command, where classification counters are displayed:

```
Device# show policy-map interface gigabitethernet1/0/1

  GigabitEthernet1/0/1

  Service-policy input: AutoQos-4.0-CiscoPhone-Input-Policy

    Class-map: AutoQos-4.0-Voip-Data-CiscoPhone-Class (match-any)
      0 packets
      Match: cos  5
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        dscp ef
      police:
          cir 128000 bps, bc 8000 bytes
        conformed 0 bytes; actions:
          transmit
        exceeded 0 bytes; actions:
          set-dscp-transmit dscp table policed-dscp
        conformed 0000 bps, exceed 0000 bps

    Class-map: AutoQos-4.0-Voip-Signal-CiscoPhone-Class (match-any)
      0 packets
      Match: cos  3
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        dscp cs3
      police:
          cir 32000 bps, bc 8000 bytes
        conformed 0 bytes; actions:
          transmit
        exceeded 0 bytes; actions:
          set-dscp-transmit dscp table policed-dscp
        conformed 0000 bps, exceed 0000 bps
    Class-map: AutoQos-4.0-Default-Class (match-any)
      0 packets
      Match: access-group name AutoQos-4.0-Acl-Default
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        dscp default

    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets, 0 bytes
        5 minute rate 0 bps

  Service-policy output: AutoQos-4.0-Output-Policy

    queue stats for all priority classes:
      Queueing
      priority level 1

      (total drops) 0
      (bytes output) 0

    Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
      0 packets
      Match:  dscp cs4 (32) cs5 (40) ef (46)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: cos  5
        0 packets, 0 bytes
        5 minute rate 0 bps
      Priority: 30% (300000 kbps), burst bytes 7500000,

      Priority Level: 1

    Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
      0 packets
      Match:  dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: cos  3
        0 packets, 0 bytes
        5 minute rate 0 bps
      Queueing
      queue-limit dscp 16 percent 80
      queue-limit dscp 24 percent 90
      queue-limit dscp 48 percent 100
      queue-limit dscp 56 percent 100

      (total drops) 0
      (bytes output) 0
      bandwidth remaining 10%

      queue-buffers ratio 10

    Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
      0 packets
      Match:  dscp af41 (34) af42 (36) af43 (38)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: cos  4
        0 packets, 0 bytes
        5 minute rate 0 bps
      Queueing
      (total drops) 0
      (bytes output) 0
      bandwidth remaining 10%
      queue-buffers ratio 10

    Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
      0 packets
      Match:  dscp af21 (18) af22 (20) af23 (22)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: cos  2
        0 packets, 0 bytes
        5 minute rate 0 bps
      Queueing

      (total drops) 0
      (bytes output) 0
      bandwidth remaining 10%
      queue-buffers ratio 10

    Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
      0 packets
      Match:  dscp af11 (10) af12 (12) af13 (14)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: cos  1
        0 packets, 0 bytes
        5 minute rate 0 bps
      Queueing

      (total drops) 0
      (bytes output) 0
      bandwidth remaining 4%
      queue-buffers ratio 10

    Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
      0 packets
      Match:  dscp cs1 (8)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Queueing

      (total drops) 0
      (bytes output) 0
      bandwidth remaining 1%
      queue-buffers ratio 10

    Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
      0 packets
      Match:  dscp af31 (26) af32 (28) af33 (30)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Queueing

      (total drops) 0
      (bytes output) 0
      bandwidth remaining 10%
      queue-buffers ratio 10

    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets, 0 bytes
        5 minute rate 0 bps
      Queueing

      (total drops) 0
      (bytes output) 0
      bandwidth remaining 25%
      queue-buffers ratio 25
```

# show rate-limit client

To configure the rate-limit for a client on the AP, use the **show rate-limit client** command.

**show rate-limit client**

## Syntax Description

This command has no arguments.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.12.1 | This command was introduced. |

The following example shows how to configure the rate-limit for a client on the AP:

```
Device# show rate-limit client
Config:
mac vap rt_rate_out rt_rate_in rt_burst_out rt_burst_in nrt_rate_out nrt_rate_in nrt_burst_out
 nrt_burst_in
00:1C:F1:09:85:E7 0 8001 8002 8003 8004 8005 8006 8007 8008
Statistics:
name up down
Unshaped 0 0
Client RT pass 0 0
Client NRT pass 0 0
Client RT drops 0 0
Client NRT drops 0 0
Per client rate limit:
mac vap rate_out rate_in policy
```

# show remote-lan all

To view the detailed output of all RLANs, use the **show remote-lan all** command.

**show remote-lan all**

## Command Default

None

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the detailed output of all RLANs:

```
Device# show remote-lan all
Remote-LAN Profile Name      : rlan_test_1
================================================
Identifier                         : 1
Status                             : Enabled
Mac-filtering                      : Not Configured
Number of Active Clients           : 1
Security_8021X                     : Disabled
8021.x Authentication list name    : Not Configured
Local Auth eap Profile Name        : Not Configured
Web Auth Security                  : Disabled
Webauth Authentication list name   : Not Configured
Web Auth Parameter Map             : Not Configured
Client association limit           : 0
Ipv4 Web Pre Auth Acl              : Not Configured
Ipv6 Web Pre Auth Acl              : Not Configured

Remote-LAN Profile Name      : rlan_test_2
================================================
Identifier                         : 2
Status                             : Enabled
Mac-filtering                      : Not Configured
Number of Active Clients           : 1
Security_8021X                     : Disabled
8021.x Authentication list name    : Not Configured
Local Auth eap Profile Name        : Not Configured
Web Auth Security                  : Disabled
Webauth Authentication list name   : Not Configured
Web Auth Parameter Map             : Not Configured
Client association limit           : 0
Ipv4 Web Pre Auth Acl              : Not Configured
Ipv6 Web Pre Auth Acl              : Not Configured
```

# show remote-lan id

To view the RLAN configuration by ID, use the **show remote-lan id** command.

**show remote-lan id** *id*

## Command Default

None

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the RLAN configuration by ID:

```
Device# show remote-lan id <id>
Remote-LAN Profile Name      : rlan_test_1
================================================
Identifier                                      : 1
Status                                          : Enabled
Mac-filtering                                   : Not Configured
Number of Active Clients                   : 1
Security_8021X                                  : Disabled
8021.x Authentication list name         : Not Configured
Local Auth eap Profile Name             : Not Configured
Web Auth Security                              : Disabled
Webauth Authentication list name      : Not Configured
Web Auth Parameter Map                   : Not Configured
Client association limit                       : 0
Ipv4 Web Pre Auth Acl                       : Not Configured
Ipv6 Web Pre Auth Acl                        : Not Configured
```

# show remote-lan name

To view the RLAN configuration by profile name, use the **show remote-lan name** command.

**show remote-lan name** *profile-name*

## Command Default

None

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the RLAN configuration by profile name:

```
Device# show remote-lan name <profile-name>
Remote-LAN Profile Name      : rlan_test_1
================================================
Identifier                          : 1
Status                              : Enabled
Mac-filtering                       : Not Configured
Number of Active Clients            : 1
Security_8021X                      : Disabled
8021.x Authentication list name     : Not Configured
Local Auth eap Profile Name         : Not Configured
Web Auth Security                   : Disabled
Webauth Authentication list name    : Not Configured
Web Auth Parameter Map              : Not Configured
Client association limit            : 0
Ipv4 Web Pre Auth Acl               : Not Configured
Ipv6 Web Pre Auth Acl               : Not Configured
```

# show remote-lan policy detail

To view the RLAN policy profile details by profile name, use the **show remote-lan policy detail** command.

**show remote-lan policy detail** *rlan_profile_name*

## Command Default

None

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the RLAN policy profile details by profile name:

```
Device# show remote-lan policy detail <rlan_profile_name>
Profile Name                    : rlan_named_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 Moniter Ingress status   : Disabled
  Flow Moniter egress status    : Disabled
Flow Monitor IPv6
  Flow Monitor Ingress Name     : Not Configured
  Flow Monitor Egress Name      : Not Configured
  Flow Moniter Ingress status   : Disabled
  Flow Moniter egress status    : Disabled
Split Tunnel Parameters
  Status                        : Disabled
  ACL name                      : Not Configured
  Override Status               : Disabled
  Gateway Address               : Not Configured
  Netmask Address               : Not Configured
DHCP
```

```
  DHCP Required                : Disabled
  DHCP Server                  : Not Configured
Accounting List                : Not Configured
```

# show remote-lan policy summary

To view the summary of policy profile for all RLANs, use the **show remote-lan policy summary** command.

**show remote-lan policy summary**

## Command Default

None

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the summary of policy profile for all RLANs:

```
Device# show remote-lan policy summary
Number of Policy Profiles: 1

Profile Name                      Description                             Status

------------------------------------------------------------------------------------------
rlan_named_pp1                 Testing RLAN policy profile                Enabled
```

# show remote-lan summary

To view the summary of all RLANs, use the **show remote-lan summary** command.

**show remote-lan summary**

## Syntax Description

This command has no arguments.

## Command Default

None

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the summary of all RLANs:

```
Device# show remote-lan summary
Number of RLANs: 1

RLAN   Profile Name                      Status
-----------------------------------------------------------------
1      rlan_test_1                       Enabled
```

# show 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see the SSH connection status:

```
Device# show ssh connection-number
```

# show tech-support wireless

To display Cisco wireless LAN controller variables frequently requested by Cisco Technical Assistance Center (TAC), use the **show tech-support wireless** command in privileged EXEC mode.

**show tech-support wireless**

## Syntax Description

This command has no arguments or keywords.

## Command Default

No default behavior or values.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

The following is sample output from the **show tech-support wireless** command:

```
Device# show tech-support wireless
 *** show ap capwap timers ***

Cisco AP CAPWAP timers

AP Discovery timer       : 10
AP Heart Beat timeout    : 30
Primary Discovery timer  : 120
Primed Join timeout      : 0
Fast Heartbeat           : Disabled
Fast Heartbeat timeout   : 1
*** show ap capwap retransmit ***
Global control packet retransmit interval : 3
Global control packet retransmit count : 5

AP Name                           Retransmit Interval             Retransmit Count
------------------------------------------------------------------------------------------
TSIM_AP-2                         3                               5
TSIM_AP-3                         3                               5
*** show ap dot11 24ghz cleanair air-quality summary ***

AQ = Air Quality
DFS = Dynamic Frequency Selection

*** show ap dot11 24ghz cleanair air-quality worst ***

AQ = Air Quality
DFS = Dynamic Frequency Selection
AP Name             Channel   Avg AQ  Min AQ  Interferers  DFS
--------------------------------------------------------------
                    0         0       0       0            No
*** show ap dot11 24ghz cleanair config ***

Clean Air Solution.............................. : Disabled
Air Quality Settings:
    Air Quality Reporting....................... : Disabled
    Air Quality Reporting Period (min).......... : 15
```

```
        Air Quality Alarms........................... : Enabled
        Air Quality Alarm Threshold.................. : 10
    Interference Device Settings:
        Interference Device Reporting................ : Enabled
            Bluetooth Link........................... : Enabled
            Microwave Oven........................... : Enabled
            802.11 FH................................ : Enabled
            Bluetooth Discovery...................... : Enabled
            TDD Transmitter.......................... : Enabled
            Jammer................................... : Enabled
            Continuous Transmitter................... : Enabled
            DECT-like Phone.......................... : Enabled
            Video Camera............................. : Enabled
            802.15.4................................. : Enabled
            WiFi Inverted............................ : Enabled
            WiFi Invalid Channel..................... : Enabled
            SuperAG.................................. : Enabled
            Canopy................................... : Enabled
            Microsoft Device......................... : Enabled
            WiMax Mobile............................. : Enabled
            WiMax Fixed.............................. : Enabled
        Interference Device Types Triggering Alarms:
            Bluetooth Link........................... : Disabled
            Microwave Oven........................... : Disabled
            802.11 FH................................ : Disabled
            Bluetooth Discovery...................... : Disabled
            TDD Transmitter.......................... : Disabled
            Jammer................................... : Disabled
            Continuous Transmitter................... : Disabled
            DECT-like Phone.......................... : Disabled
            Video Camera............................. : Disabled
      802.15.4................................. : Disabled
            WiFi Inverted............................ : Enabled
            WiFi Invalid Channel..................... : Enabled
            SuperAG.................................. : Disabled
            Canopy................................... : Disabled
            Microsoft Device......................... : Disabled
            WiMax Mobile............................. : Disabled
            WiMax Fixed.............................. : Disabled
        Interference Device Alarms................... : Enabled
    Additional Clean Air Settings:
        CleanAir Event-driven RRM State.............. : Disabled
        CleanAir Driven RRM Sensitivity.............. : LOW
        CleanAir Persistent Devices state............ : Disabled
```

# show tech-support wireless ap

To display specific information about the Cisco APs variables frequently requested by Cisco Technical Assistance Center (TAC), use the **show tech-support wireless ap** command in privileged EXEC mode.

**show tech-support wireless ap**

### Syntax Description

This command has no arguments or keywords.

### Command Default

None

### Command Modes

Privileged EXEC (#)

### Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

### Usage Guidelines

The output of the following commands are displayed as part of **show tech-support wireless ap**command:

- show ap session termination statistics
- show ap status
- show ap tag summary
- show platform software bssid chassis active F0 statistics
- show platform software bssid chassis active R0 statistics
- show platform software capwap chassis active F0 statistics
- show platform software capwap chassis active R0 statistics
- show platform software dtls chassis active F0 statistics
- show platform software dtls chassis active R0 statistics
- show platform software radio chassis active F0 statistics
- show platform software radio chassis active R0 statistics

### Example

The following is sample output from the **show tech-support wireless ap** command

```
Device# show tech-support wireless ap

------------------ show platform software dtls chassis active R0 statistics ------------------


DTLS Counters     (Success/Failure)
-----------------------------------
Create                  0/0
```

```
Delete                  0/0

Switch 1:
OM Create               0/0
OM Delete               0/0
Ack Nack Notify         0/0


------------------ show platform software radio chassis active R0 statistics
------------------



Switch 1:
NACK Notify             0/0
  Create Failure        0
  Delete Failure        0


------------------ show platform software bssid chassis active R0 statistics
------------------



Switch 1:
NACK Notify             0/0
  Create Failure        0
  Delete Failure        0


------------------ show platform software capwap chassis active R0 statistics
------------------


Capwap Counters   (Success/Failure)
-----------------------------------
Create                  0/0
Delete                  0/0
Modify                  0/0

Switch 1:
OM Create               0/0
OM Delete               0/0
ACK-NACK Notify         0/0
  Tunnel State          0/0
  Tunnel Create         0/0
  Tunnel Modify         0/0
  Tunnel Delete         0/0


------------------ show platform software dtls chassis active F0 statistics ------------------


DTLS Counters     (Success/Failure)
-----------------------------------
Create                  0/0
Delete                  0/0
HW Create               0/0
HW Modify               0/0
HW Delete               0/0
Create Ack              0/0
Modify Ack              0/0
Delete Ack              0/0
Ack Ack Notify          0/0
Ack Nack Notify         0/0
Nack Notify             0/0
HA Seq GET              665/0
HA Seq SET              0/0
HA Seq Crypto GET       0/0
HA Seq Crypto SET       0/0
HA Seq Crypto Callback  0/0

HA Seq last Responsed   0
HA Seq Pending          0
HA Seq Outstanding cb   0


------------------ show platform software radio chassis active F0 statistics
------------------


Radio Counters    (Success/Failure)
-----------------------------------
Create                  0/0
Delete                  0/0
HW Create               0/0
HW Modify               0/0
HW Delete               0/0
Create Ack              0/0
Modify Ack              0/0
Delete Ack              0/0
Nack Notify             0/0


------------------ show platform software bssid chassis active F0 statistics
------------------


Bssid Counters    (Success/Failure)
-----------------------------------
Create                 0/0
Delete                 0/0
HW Create              0/0
HW Modify              0/0
HW Delete              0/0
Create Ack             0/0
Modify Ack             0/0
Delete Ack             0/0
Nack Notify            0/0


------------------ show platform software capwap chassis active F0 statistics
------------------


Capwap Counters   (Success/Failure)
-----------------------------------
Create                  0/0
Delete                  0/0
HW Create               0/0
HW Modify               0/0
HW Delete               0/0
Create Ack              0/0
Modify Ack              0/0
Delete Ack              0/0
Ack Ack Notify          0/0
Ack Nack Notify         0/0
Nack Notify             0/0
```

```
------------------ show ap auto-rf dot11 24ghz ------------------


------------------ show ap auto-rf dot11 5ghz ------------------


------------------ show ap capwap retransmit ------------------


------------------ show ap config dot11 dual-band summary ------------------


------------------ show ap config general ------------------



------------------ show ap dot11 24ghz channel ------------------


Leader Automatic Channel Assignment
  Channel Assignment Mode                    : AUTO
  Channel Update Interval                    : 600 seconds
  Anchor time (Hour of the day)              : 0
  Channel Update Contribution
    Noise                                    : Enable
    Interference                             : Enable
    Load                                     : Disable
    Device Aware                             : Disable
  CleanAir Event-driven RRM option           : Disabled
  Channel Assignment Leader                  : ewlc-doc (9.12.32.10)
  Last Run                                   : 25 seconds ago

  DCA Sensitivity Level                      : MEDIUM : 10 dB
  DCA Minimum Energy Limit                   : -95 dBm
  Channel Energy Levels
    Minimum                                  : unknown
    Average                                  : unknown
    Maximum                                  : -128 dBm
  Channel Dwell Times
    Minimum                                  : unknown
    Average                                  : unknown


------------------ show ap dot11 24ghz group ------------------


Radio RF Grouping

  802.11b Group Mode               : AUTO
  802.11b Group Update Interval    : 600 seconds
  802.11b Group Leader             : ewlc-doc (9.12.32.10)
  802.11b Last Run                 : 26 seconds ago


RF Group Members

Controller name                   Controller IP
```

```
--------------------------------------------------
ewlc-doc                          9.12.32.10



------------------ show ap dot11 24ghz load-info ------------------



------------------ show ap dot11 24ghz monitor ------------------


Default 802.11b AP monitoring
  802.11b Monitor Mode                 : Enabled
  802.11b Monitor Channels             : Country channels
  802.11b RRM Neighbor Discover Type   : Transparent
  802.11b AP Coverage Interval         : 180 seconds
  802.11b AP Load Interval             : 60 seconds
  802.11b AP Noise Interval            : 180 seconds
  802.11b AP Signal Strength Interval  : 60 seconds
  802.11b NDP RSSI Normalization       : Enabled


------------------ show ap dot11 24ghz network ------------------



802.11b Network                           : Enabled
11gSupport                                : Enabled
11nSupport                                : Enabled
802.11b/g Operational Rates
  802.11b 1M                              : Mandatory
  802.11b 2M                              : Mandatory
  802.11b 5.5M                            : Mandatory
  802.11b 11M                             : Mandatory
  802.11g 6M                              : Supported
  802.11g 9M                              : Supported
  802.11g 12M                             : Supported
  802.11g 18M                             : Supported
  802.11g 24M                             : Supported
  802.11g 36M                             : Supported
  802.11g 48M                             : Supported
  802.11g 54M                             : Supported
802.11n MCS Settings:
  MCS 0 : Supported
  MCS 1 : Supported
  MCS 2 : Supported
  MCS 3 : Supported


------------------ show ap dot11 24ghz profile ------------------



Default 802.11b AP performance profiles
  802.11b Global Interference threshold    : 10 %
  802.11b Global noise threshold           : -70 dBm
  802.11b Global RF utilization threshold  : 80 %
  802.11b Global throughput threshold      : 1000000 bps
  802.11b Global clients threshold         : 12 clients


------------------ show ap dot11 24ghz summary ------------------
```

```
------------------ show ap dot11 24ghz txpower ------------------


Automatic Transmit Power Assignment

Transmit Power Assignment Mode          : AUTO
Transmit Power Update Interval          : 600 seconds
Transmit Power Threshold                : -70 dBm
Transmit Power Neighbor Count           : 3 APs
Min Transmit Power                      : -10 dBm
Max Transmit Power                      : 30 dBm
Update Contribution
    Noise                               : Enable
    Interference                        : Enable
    Load                                : Disable
    Device Aware                        : Disable
Transmit Power Assignment Leader        : ewlc-doc (9.12.32.10)
Last Run                                : 27 seconds ago


------------------ show ap dot11 5ghz channel ------------------


Leader Automatic Channel Assignment
  Channel Assignment Mode                    : AUTO
  Channel Update Interval                    : 600 seconds
  Anchor time (Hour of the day)              : 0
  Channel Update Contribution
    Noise                                    : Enable
    Interference                             : Enable
    Load                                     : Disable
    Device Aware                             : Disable
  CleanAir Event-driven RRM option           : Disabled
  Channel Assignment Leader                  : ewlc-doc (9.12.32.10)
  Last Run                                   : 27 seconds ago

  DCA Sensitivity Level                      : MEDIUM : 15 dB
  DCA 802.11n/ac Channel Width               : 20 MHz
  DCA Minimum Energy Limit                   : -95 dBm
  Channel Energy Levels
    Minimum                                  : unknown
    Average                                  : unknown
    Maximum                                  : -128 dBm
  Channel Dwell Times
    Minimum                                  : unknown


------------------ show ap dot11 5ghz group ------------------


Radio RF Grouping

  802.11a Group Mode               : AUTO
  802.11a Group Update Interval    : 600 seconds
  802.11a Group Leader             : ewlc-doc (9.12.32.10)
  802.11a Last Run                 : 28 seconds ago


RF Group Members

Controller name                  Controller IP
```

```
--------------------------------------------------
ewlc-doc                          9.12.32.10




------------------ show ap dot11 5ghz load-info ------------------



------------------ show ap dot11 5ghz monitor ------------------


Default 802.11a AP monitoring
  802.11a Monitor Mode                 : Enabled
  802.11a Monitor Channels             : Country channels
  802.11a RRM Neighbor Discover Type   : Transparent
  802.11a AP Coverage Interval         : 180 seconds
  802.11a AP Load Interval             : 60 seconds
  802.11a AP Noise Interval            : 180 seconds
  802.11a AP Signal Strength Interval  : 60 seconds
  802.11a NDP RSSI Normalization       : Enabled


------------------ show ap dot11 5ghz network ------------------



802.11a Network                           : Enabled
11nSupport                                : Enabled
  802.11a Low Band                        : Enabled
  802.11a Mid Band                        : Enabled
  802.11a High Band                       : Enabled
802.11a Operational Rates
  802.11a 6M                              : Mandatory
  802.11a 9M                              : Supported
  802.11a 12M                             : Mandatory
  802.11a 18M                             : Supported
  802.11a 24M                             : Mandatory
  802.11a 36M                             : Supported
  802.11a 48M                             : Supported
  802.11a 54M                             : Supported
802.11n MCS Settings:
  MCS 0 : Supported
  MCS 1 : Supported
  MCS 2 : Supported
  MCS 3 : Supported
  MCS 4 : Supported
  MCS 5 : Supported


------------------ show ap dot11 5ghz profile ------------------


Default 802.11a AP performance profiles

  802.11a Global Interference threshold          : 10 %
  802.11a Global noise threshold                  : -70 dBm
  802.11a Global RF utilization threshold        : 80 %
  802.11a Global throughput threshold             : 1000000 bps
  802.11a Global clients threshold                : 12 clients


------------------ show ap dot11 5ghz summary ------------------
```

```
------------------ show ap dot11 5ghz txpower ------------------


Automatic Transmit Power Assignment

Transmit Power Assignment Mode          : AUTO
Transmit Power Update Interval          : 600 seconds
Transmit Power Threshold                : -70 dBm
Transmit Power Neighbor Count           : 3 APs
Min Transmit Power                      : -10 dBm
Max Transmit Power                      : 30 dBm
Update Contribution
    Noise                               : Enable
    Interference                        : Enable
    Load                                : Disable
    Device Aware                        : Disable
Transmit Power Assignment Leader        : ewlc-doc (9.12.32.10)
Last Run                                : 28 seconds ago


------------------ show ap image ------------------




------------------ show wireless stats ap join summary ------------------

Number of APs: 0

Base MAC        Ethernet MAC    AP Name                           IP Address       Status
     Last Failure Type     Last Disconnect Reason
------------------------------------------------------------------------------------------


------------------ show ap rf-profile summary ------------------



Number of RF-profiles: 6

RF Profile Name                  Band     Description                          State
------------------------------------------------------------------------------------
Low_Client_Density_rf_5gh        5 GHz    pre configured Low Client Density rf Up
High_Client_Density_rf_5gh       5 GHz    pre configured High Client Density r Up
Low_Client_Density_rf_24gh       2.4 GHz  pre configured Low Client Density rf Up
High_Client_Density_rf_24gh      2.4 GHz  pre configured High Client Density r Up
Typical_Client_Density_rf_5gh    5 GHz    pre configured Typical Density rfpro Up
Typical_Client_Density_rf_24gh   2.4 GHz  pre configured Typical Client Densit Up


------------------ show ap slots ------------------



------------------ show ap summary ------------------


Number of APs: 0
```

```
------------------ show ap uptime ------------------


Number of APs: 0


------------------ show ap tag summary ------------------


Number of APs: 0


------------------ show ap status ------------------


------------------ show ap cdp neighbors ------------------


Number of neighbors: 0


------------------ show ap ap-join-profile summary ------------------


Number of AP Profiles: 1
AP Profile Name                   Description
------------------------------------------------------------------------
default-ap-profile                default ap profile

------------------ show ap link-encryption ------------------


------------------ show wireless stats ap session termination ------------------


------------------ show wireless loadbalance ap affinity wncd 0 ------------------


------------------ show wireless loadbalance ap affinity wncd 1 ------------------


------------------ show wireless loadbalance ap affinity wncd 2 ------------------


------------------ show wireless loadbalance ap affinity wncd 3 ------------------


------------------ show wireless loadbalance ap affinity wncd 4 ------------------


------------------ show wireless loadbalance ap affinity wncd 5 ------------------
```

```
------------------ show wireless loadbalance ap affinity wncd 6 ------------------


------------------ show wireless loadbalance ap affinity wncd 7 ------------------
```

# show tech-support wireless client

To print the data related to all clients or a particular client, use the **show tech-support wireless client** command in privileged EXEC mode.

**show tech-support wireless client**

## Syntax Description

| | |
|---|---|
| **mac-address** | Client MAC address. |

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

The output of the following commands are displayed as part of **show tech-support wireless client** command:

- show platform software wireless-client chassis active F0 statistics
- show platform software wireless-client chassis active R0 statistics
- show wireless client calls active
- show wireless client calls rejected
- show wireless client client-statistics summary
- show wireless client device summary
- show wireless client mac <mac-addr> details
- show wireless client probing
- show wireless client sleeping-client
- show wireless client statistic
- show wireless client steering
- show wireless client summary
- show wireless exclusionlist
- show wireless pmk-cache

# show tech-support wireless datapath

To print the data related to CPP datapath, use the **show tech-support wireless datapath** command in privileged EXEC mode.

**show tech-support wireless datapath**

## Syntax Description

This command has no keywords or arguments.

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

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

- show platform hardware chassis active qfp feature wireless ipsg cpp-client table ipv4 all
- show platform hardware chassis active qfp feature wireless ipsg cpp-client table ipv6 all
- show platform hardware chassis active qfp feature wireless ipsg datapath statistics global
- show platform hardware chassis active qfp feature wireless ipsg datapath table ipv4 all
- show platform hardware chassis active qfp feature wireless ipsg datapath table ipv6 all
- show platform hardware chassis active qfp feature wireless mgmt-intf cpp-client summary
- show platform hardware chassis active qfp feature wireless mgmt-intf datapath summary
- show platform hardware chassis active qfp feature wireless punt statistics
- show platform hardware chassis active qfp feature wireless wlan summary
- show platform hardware chassis active qfp feature wireless wlclient cpp-client statistics
- show platform hardware chassis active qfp feature wireless wlclient cpp-client summary
- show platform hardware chassis active qfp feature wireless wlclient datapath statistic drop
- show platform hardware chassis active qfp feature wireless wlclient datapath summary
- show platform hardware chassis active qfp feature wireless wlclient datapath table dataglean all
- show platform hardware chassis active qfp infrastructure punt statistics type per-cause
- show platform hardware chassis active qfp statistics drop
- show platform software bssid chassis active F0
- show platform software bssid chassis active F0 statistics
- show platform software capwap chassis active F0
- show platform software capwap chassis active F0 statistics
- show platform software dtls chassis active F0
- show platform software dtls chassis active F0 statistics
- show platform software wireless-client chassis active F0
- show platform software wireless-client chassis active F0 statistics
- show platform software wlan chassis active F0

In the presence of standby node, the following datapath commands are also displayed:

- show platform hardware chassis standby qfp feature wireless bssid summary
- show platform hardware chassis standby qfp feature wireless capwap cpp-client statistics
- show platform hardware chassis standby qfp feature wireless capwap cpp-client summary
- show platform hardware chassis standby qfp feature wireless capwap datapath statistics drop
- show platform hardware chassis standby qfp feature wireless capwap datapath statistics fragmentation
- show platform hardware chassis standby qfp feature wireless capwap datapath statistics reassembly

- show platform hardware chassis standby qfp feature wireless capwap datapath summary
- show platform hardware chassis standby qfp feature wireless dtls cpp-client statistics
- show platform hardware chassis standby qfp feature wireless dtls cpp-client summary
- show platform hardware chassis standby qfp feature wireless dtls datapath statistics
- show platform hardware chassis standby qfp feature wireless dtls datapath summary
- show platform hardware chassis standby qfp feature wireless halo statistics
- show platform hardware chassis standby qfp feature wireless ipsg cpp-client statistics
- show platform hardware chassis standby qfp feature wireless ipsg cpp-client table ipv4 all
- show platform hardware chassis standby qfp feature wireless ipsg cpp-client table ipv6 all
- show platform hardware chassis standby qfp feature wireless ipsg datapath statistics global
- show platform hardware chassis standby qfp feature wireless ipsg datapath table ipv4 all
- show platform hardware chassis standby qfp feature wireless ipsg datapath table ipv6 all
- show platform hardware chassis standby qfp feature wireless mgmt-intf cpp-client summary
- show platform hardware chassis standby qfp feature wireless mgmt-intf datapath summary
- show platform hardware chassis standby qfp feature wireless punt statistics
- show platform hardware chassis standby qfp feature wireless wlan summary
- show platform hardware chassis standby qfp feature wireless wlclient cpp-client statistics
- show platform hardware chassis standby qfp feature wireless wlclient cpp-client summary
- show platform hardware chassis standby qfp feature wireless wlclient datapath statistic drop
- show platform hardware chassis standby qfp feature wireless wlclient datapath summary
- show platform hardware chassis standby qfp feature wireless wlclient datapath table dataglean all
- show platform hardware chassis standby qfp statistics drop
- show platform software bssid chassis standby F0
- show platform software bssid chassis standby F0 statistics
- show platform software capwap chassis standby F0
- show platform software capwap chassis standby F0 statistics
- show platform software dtls chassis standby F0
- show platform software dtls chassis standby F0 statistics
- show platform software wireless-client chassis standby F0
- show platform software wireless-client chassis standby F0 statistics
- show platform software wlan chassis standby F0

### Example

The following is sample output from the **show tech-support wireless datapath** command

```
Device# show tech-support wireless datapath


------------------ show platform hardware chassis active qfp statistics drop
------------------

-------------------------------------------------------------------------
Global Drop Stats                         Packets                  Octets
-------------------------------------------------------------------------
Disabled                                    22230                 2045194
InvL2Hdr                                  4765368               744492240
Ipv4NoAdj                                       6                     736
Ipv4NoRoute                                    18                    2358
Ipv6mcNoRoute                                   3                     270
SWPortDrop                                  14432                 2886027
SWPortSrcFilter                             53265                53992718
SWPortStpState                              42041                 3269790
SWPortVlanNotCfg                          5515542               674079804
SwitchL2m                                      78                   10062
SwitchL2mIGMP                               18866                 1283348
SwitchL2mUnconfigWireless                      78                   11622
WlsCapwapNoTunnel                               3                     627


------------------ show platform hardware chassis active qfp feature wireless punt statistics
 ------------------


CPP Wireless Punt stats:

                                 App Tag     Packet Count
                                 -------     ------------
         CAPWAP_PKT_TYPE_DOT11_PROBE_REQ                0
              CAPWAP_PKT_TYPE_DOT11_MGMT               56
              CAPWAP_PKT_TYPE_DOT11_IAPP            22177
              CAPWAP_PKT_TYPE_DOT11_RFID                0
               CAPWAP_PKT_TYPE_DOT11_RRM                0
             CAPWAP_PKT_TYPE_DOT11_DOT1X                0
        CAPWAP_PKT_TYPE_CAPWAP_KEEPALIVE                0
      CAPWAP_PKT_TYPE_MOBILITY_KEEPALIVE                0
            CAPWAP_PKT_TYPE_CAPWAP_CNTRL           303661
             CAPWAP_PKT_TYPE_CAPWAP_DATA                0
          CAPWAP_PKT_TYPE_MOBILITY_CNTRL                0
                         WLS_SMD_WEBAUTH                0
                       SISF_PKT_TYPE_ARP              303
                      SISF_PKT_TYPE_DHCP              282
                     SISF_PKT_TYPE_DHCP6                0
                   SISF_PKT_TYPE_IPV6_ND                0
                SISF_PKT_TYPE_DATA_GLEAN                0
             SISF_PKT_TYPE_DATA_GLEAN_V6                0
                SISF_PKT_TYPE_DHCP_RELAY                0
         CAPWAP_PKT_TYPE_CAPWAP_RESERVED                0


------------------ show platform hardware chassis active qfp infrastructure punt statistics
 type per-cause ------------------

Global Per Cause Statistics
```

```
  Number of punt causes =   136

  Per Punt Cause Statistics
                                                         Packets              Packets
  Counter ID  Punt Cause Name                            Received             Transmitted

-----------------------------------------------------------------------------------------

  000         Reserved                                   0                    0

  001         MPLS ICMP Can't Fragment                   0                    0

  002         IPv4 Options                               0                    0

  003         Layer2 control and legacy                  0                    0

  004         PPP Control                                0                    0

  005         CLNS IS-IS Control                         0                    0

  006         HDLC keepalives                            0                    0

  007         ARP request or response                    2687                 2687

  008         Reverse ARP request or repsonse            0                    0

  009         Frame-relay LMI Control                    0                    0

  010         Incomplete adjacency                       0                    0

  011         For-us data                                0                    0

  012         Mcast Directly Connected Source            0                    0

  013         Mcast IPv4 Options data packet             0                    0

  014         Skip egress processing                     0                    0

  015         MPLS TTL expired                           0                    0

  016         MPLS Reserved label (ie: 0-15)             0                    0

  017         IPv6 Bad hop limit                         0                    0

  018         IPV6 Hop-by-hop Options                    0                    0

  019         Mcast Internal Copy                        0                    0

  020         Generic QFP generated packet               0                    0

  021         RP<->QFP keepalive                         46691                46691

  022         QFP Fwall generated packet                 0                    0

  023         Mcast IGMP Unroutable                      0                    0

  024         Glean adjacency                            2557                 2556

  025         Mcast PIM signaling                        0                    0

  026         QFP ICMP generated packet                  0                    0

  027         Subscriber session control                 0                    0
```

```
028         Subscriber data switching back            0                      0
029         RP handled ICMP                           0                      0
030         RP injected For-us data                   0                      0
031         Punt adjacency                            0                      0
032         SBC RTP DTMF                              0                      0
033         Pseudowire VCCV control channel           0                      0
034         Generic QFP generated packet (keep GPM)   0                      0
035         Ethernet slow protocol (ie: LACP, OAM)    0                      0
036         Ethernet OAM Loopback                     0                      0
037         UNUSED                                    0                      0
038         SPA IPC packet                            0                      0
039         Punt and replicate                        0                      0
040         PPPoE control                             0                      0
041         PPPoE session                             0                      0
042         L2TP control                              0                      0
043         IP Subscriber control (ie: FSOL, keepali  0                      0
044         L2TP session                              0                      0
045         BFD control                               0                      0
046         MVPN non-RPF signaling packet             0                      0
047         MVPN PIM signalling packet                0                      0
048         Mcast punt to RP                          0                      0
049         SBC generated packet                      0                      0
050         IPv6 packet                               0                      0
051         DMVPN NHRP redirect                       0                      0
052         PFR monitored prefix logging              0                      0
053         PFR top talkers logging                   0                      0
054         PFR top talkers application logging       0                      0
055         For-us control                            0                      0
056         RP injected for-us control                0                      0
057         QFP VTCP generated packet                 0                      0
058         Layer2 bridge domain data packet          0                      0
059         QFP Stile generated packet                0                      0
```

```
060         IP subnet or broadcast packet            167                 167
061         Ethernet CFM packet                      0                   0
062         Ethernet CFM notify packet               0                   0
063         LISP LSB NOTIFICATION                    0                   0
064         Service Engine packet                    0                   0
065         L2BD Control packet from FIA             0                   0
066         L2BD Control Message from CPP            0                   0
067         MFR_LIP_CONTROL                          0                   0
068         Media Monitoring record punted from CPP  0                   0
069         OTV Control packet                       0                   0
070         OTV ARP packet                           0                   0
071         REP control                              0                   0
072         IP MTU EXCEPTION                         0                   0
073         STP BPDU's                               186832              186832
074         ACL log                                  0                   0
075         EPC                                      0                   0
076         Lisp Dynamic eid                         0                   0
077         L2 Control packet                        122389              122389
078         WAAS CPP to CPP punt                     0                   0
079         dhcp snoop                               0                   0
080         Metric Mediation Agent record punted fro 0                   0
081         IPv6 DMVPN NHRP redirect                 0                   0
082         Ethernet CFM packet from core            0                   0
083         Ethernet CFM punt fwd packet             0                   0
084         PTP punt fwd packet                      0                   0
085         ISDN D-Channel raw packet                0                   0
086         Service controller SCG punt pkt          0                   0
087         IPv6 FHS SG dropped packet               0                   0
088         IPv6 FHS Data glean packet               0                   0
089         SBC DSP pkts                             0                   0
090         Raw Socket Data packet                   0                   0
091         SSLVPN session control                   0                   0
```

```
092         ICMP 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 pack  0                     0
096         Layer2 control protocols                  0                     0
097         Packets to LFTS                           22177                 22177
098         VLAN Auto Sense FSOL                      0                     0
099         ZTP Discovery packet                      0                     0
100         cable arp filter                          0                     0
101         Cable L3 mobility                         0                     0
102         Source Verify inconclusive                0                     0
103         cable modem pre reg                       0                     0
104         mpls receive adj                          0                     0
105         MKA EAPoL packet                          0                     0
106         ICMP Unreachable                          0                     0
107         Cable DHCP                                0                     0
108         Snooping packet                           0                     0
109         snoop packets                             0                     0
110         msg Indicating ppp intf assigned ip addr  0                     0
111         msg indicating there is another common h  0                     0
112         QoS CAC Flow Report                       0                     0
113         Active identity                           0                     0
114         BGP Overlay Tunnel packet                 0                     0
115         Lisp gsmr enabled                         0                     0
116         Async TS                                  0                     0
117         Metric Mediation Agent Packet             0                     0
118         Cable DHCPV6 Solicit                      0                     0
119         Cable DHCPV6 Request                      0                     0
120         SBC RTP FWD DTMF                          0                     0
121         Path Manager                              0                     0
122         L2 LISP VXLAN                             0                     0
123         dialer-list                               0                     0
```

```
  124         Dialer update time                        0                     0

  125         Cable RPHY CTRL                           0                     0

  126         OpenFlow SDN                              0                     0

  127         Path Manager TTL expired                  0                     0

  128         L3 PTP message                            0                     0

  129         wls 802.11 Packets to LFTS                56                    56

  130         wls CAPWAP Packets to LFTS                303661                303661

  131         wls MOBILITY Packets to LFTS              0                     0

  132         wls SISF Packets to LFTS                  585                   585

  133         cable DHCPv6 subscriber-side              0                     0

  134         cable DHCPv4 subscriber-side              0                     0

  135         cable DHCPv4 sub-side disc/req            0                     0


  Number of inject causes = 49

  Per Inject Cause Statistics
                                                        Packets               Packets
  Counter ID  Inject Cause Name                         Received              Transmitted

------------------------------------------------------------------------------------------

  000         RESERVED                                  0                     0

  001         L2 control/legacy                         3115                  3115

  002         QFP destination lookup                    0                     0

  003         QFP IPv4/v6 nexthop lookup                0                     0

  004         QFP generated packet                      0                     0

  005         QFP <->RP keepalive                       46691                 0

  006         QFP Fwall generated packet                0                     0

  007         QFP adjacency-id lookup                   0                     0

  008         Mcast specific inject packet              0                     0

  009         QFP ICMP generated packet                 0                     0

  010         QFP/RP->QFP Subscriber data packet        0                     0

  011         SBC DTMF                                  0                     0

  012         ARP request or response                   3637                  3637

  013         Ethernet OAM loopback packet              0                     0
```

```
014         UNUSED                                    0                     0

015         PPPoE discovery packet                    0                     0

016         PPPoE session packet                      0                     0

017         QFP inject for pp_index lookup            0                     0

018         QFP inject replicate                      0                     0

019         QFP inject PIT lookup                     0                     0

020         SBC generated packets                     0                     0

021         QFP VTCP generated packet                 0                     0

022         QFP Stile generated packet                0                     0

023         Service Engine generated packet           0                     0

024         Layer2 frame to EFP                       0                     0

025         Layer2 frame to BD                        0                     0

026         QfP Asym Routing redirected pkt           0                     0

027         Compressed packet from WAAS               0                     0

028         Media (e.g. voice) associated with a ses  0                     0

029         service controller scg packet             0                     0

030         Packet for 14 port Serial IM              0                     0

031         Subscriber generated TCP reset packet     0                     0

032         Layer2 frame to INPUT EFP                 0                     0

033         SSLVPN inject control                     0                     0

034         injected packet from UTD SP               0                     0

035         injected packet from DPSS SN              0                     0

036         injected packet by AppNav vPath           0                     0

037         Uncompressed packet from WAAS             0                     0

038         Autonomic Network Channel Discovery pack  0                     0

039         Cable Bundle Flood Inject                 0                     0

040         Cable L2 unicast inject                   0                     0

041         downstream jib packet                     0                     0

042         switch port layer 2 control packet        6254                  6253

043         Applications Injecting Pkts using LFTS    303874                303269

044         Enhanced ping and traceroute              0                     0

045         Applications Injecting packets with SGT   0                     0
```

```
  046         CoPP packets from EPC_WS                0                 0

  047         Async TS                                0                 0

  048         Layer2 frame to VLAN                    0                 0


------------------ show platform hardware chassis active qfp feature wireless mgmt-intf
cpp-client summary ------------------

Wireless Management Interface Info
 CPP IF_H   VLAN   MAC Address
--------------------------------
   0XF       78   001e.1405.2bff


------------------ show platform hardware chassis active qfp feature wireless mgmt-intf
datapath summary ------------------

Wireless Management Interface Info
IF_H       VLAN   MAC Address
--------------------------------------
0xF        78     001e.1405.2bff


------------------ show platform software wlan chassis active F0 ------------------


WLAN Interface ID  WLAN ID     WLAN Name                                 AOM ID  Status

------------------------------------------------------------------------------------------

0xf0400001         1           att                                          275  Done

0xf0400002         2           verizon                                      292  Done



------------------ show platform hardware chassis active qfp feature wireless wlan summary
 ------------------

CPP Wlan Database Summary
Total number of wlan interfaces : 2
         if_name             cpp_if_hdl    pal_if_hdl     in_uidb       out_uidb
        ssid
------------------------------------------------------------------------------------------

   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
HW Modify              0/0
HW Delete              0/0
Create Ack             0/0
Modify Ack             0/0
Delete Ack             0/0
Nack Notify            0/0


------------------ show platform software bssid chassis active F0 ------------------



------------------ show platform hardware chassis active qfp feature wireless bssid summary
 ------------------



------------------ show platform software capwap chassis active F0 statistics
------------------


Capwap Counters   (Success/Failure)
-----------------------------------
Create                  424/0
Delete                  420/0
HW Create               424/0
HW Modify               0/0
HW Delete               420/0
Create Ack              424/0
Modify Ack              0/0
Delete Ack              420/0
Ack Ack Notify          0/0
Ack Nack Notify         0/0
Nack Notify             0/0

------------------ show platform software capwap chassis active F0 ------------------


 Tunnel ID  AP MAC          Type            IP                Port      AOM ID  Status

------------------------------------------------------------------------------------------

0x90000042  00a8.2200.0200  Data            78.1.50.1        52345        3271  Done

0xa0000002  0000.0000.0000  Mobility Data   78.1.1.23        16667        1426  Done

0xa0000003  0000.0000.0000  Mobility Data   78.1.1.24        16667        1427  Done

0xa0000004  0000.0000.0000  Mobility Data   78.1.1.25        16667        1428  Done




------------------ show platform hardware chassis active qfp feature wireless capwap
cpp-client statistics ------------------


CAPWAP cpp-client plumbing statistics
Number Msg in = ack + nak + ack fail + nak fail + errors

Counter                                        Value
--------------------------------------------------------------------
Create from fp                                 424
```

```
Modify from fp                                 0
Delete from fp                                 420
Create ack to fp                               424
Create ack fail to fp                          0
Create nack to fp                              0
Create nack fail to fp                         0
Modify ack to fp                               0
Modify ack fail to fp                          0
Modify nack to fp                              0
Modify nack fail to fp                         0
Delete ack to fp                               420
Delete ack fail to fp                          0
Delete nack to fp                              0
Delete nak fail to fp                          0


------------------ show platform hardware chassis active qfp feature wireless capwap
cpp-client summary ------------------

 cpp_if_hdl    pal_if_hdl       AP MAC           Src IP            Dst IP       Dst Port
Tun Type
------------------------------------------------------------------------------------------

   0X108       0X90000042   00a8.2200.0200      78.1.1.7         78.1.50.1       52345
  DATA
   0X10B       0XA0000002   0000.0000.0000      78.1.1.7         78.1.1.23       16667
MOBILITY
   0X10C       0XA0000003   0000.0000.0000      78.1.1.7         78.1.1.24       16667
MOBILITY
   0X10D       0XA0000004   0000.0000.0000      78.1.1.7         78.1.1.25       16667
MOBILITY


------------------ show platform hardware chassis active qfp feature wireless capwap datapath
 summary ------------------


Vrf Src Port Dst IP          Dsp Port Input Uidb Output Uidb Instance Id
--- -------- ------          -------- ---------- ----------- -----------
0   16667    78.1.1.25       16667    95733      95731       0
0   5247     78.1.50.1       52345    95738      95736       3
0   16667    78.1.1.24       16667    95734      95732       0
0   16667    78.1.1.23       16667    95735      95733       0


------------------ show platform hardware chassis active qfp feature wireless capwap datapath
 statistics drop ------------------



Drop Cause                                                                Packets
      Octets
================================================================================
====================
Wls Capwap unsupported link type Error                                          0
           0
Wls Capwap invalid tunnel Error                                                 0
           0
Wls Capwap input config missing Error                                           0
           0
Wls Capwap invalid TPID Error                                                   0
           0
Wls Capwap ingress parsing Error                                                0
           0
```

```
Wls Capwap invalid FC subtype Error                                             0
           0
Wls Capwap SNAP Invalid HLEN Error                                              0
           0
Wls Client V6 Max Address Error                                                 0
           0


------------------ show platform hardware chassis active qfp feature wireless capwap datapath
 statistics fragmentation ------------------


CPP Wireless Fragmentation stats:

                             Description         Packet Count          Octet Count

                             -----------         ------------          -----------
 Capwap Packets to be Fragmented (RX)                       0                    0
 Capwap Fragments to be Recycled                            0                    0
 Capwap Fragments Recycled (TX)                             0                    0
 Error: Original Packet Too Big                             0                    0
 Error: CAPWAP MTU Not Valid                                0                    0
 Error: Recycle Queue Full                                  0                    0
 Error: Recycle Queue Not Valid                             0                    0
 Error: GPM Memory Init Failure                             0                    0
 Error: Multipass Requeue Failure                           0                    0


------------------ show platform hardware chassis active qfp feature wireless capwap datapath
 statistics reassembly ------------------


CPP Wireless Reassembly Memory stats:

                             Description            Count
                             -----------            -----
                         Free info chunk            32768
                   Allocated info chunks            32768
                    Free fragment chunks           131072
               Allocated fragment chunks           131072


CPP Wireless Reassembly Packet stats: (outstanding pkt_cnt 0)

                             Description     Packet Count      Octet Count
                             -----------     ------------      -----------
     Capwap Reassembled Packets                         0                0
     Capwap Fragments Received                          0                0
     Capwap Fragments Consumed (Saved)                  0                0
     Capwap Fragments Dropped                           0                0
     Capwap Reassembly Timeouts                         0                0
     Error - Early-drop fragments                       0                0
     Error - Invalid packet size                        0                0
     Error - Fragment size too big                      0                0
     Error - Too many fragments                         0                0
     Error - Overlap offset fragments                   0                0
     Error - Duplicated fragments                       0                0
     Error - Allocate info chunk memory                 0                0
     Error - Allocate frag chunk memory                 0                0
     Error - Hash bucket threshold                      0                0
     Error - Cannot save and gather pkts                0                0
     Error - Get recycle reass_info NULL                0                0
     Error - BQS memory alloc NULL                      0                0
     Error - BQS memory free NULL                       0                0
     DEBUG - # of lock sync aquired                    2                2
     DEBUG - # of lock released                        2                2
     DEBUG - CPP_CW_BQS_MX_ALLOC #                     0                0
     DEBUG - CPP_CW_BQS_MX_FREE  #                     0                0
     DEBUG - CPP_REASS_INFO_ALLOC #                    0                0
     DEBUG - CPP_REASS_INFO_FREE  #                    0                0
     DEBUG - CPP_REASS_FRAG_ALLOC #                    0                0
     DEBUG - CPP_REASS_FRAG_FREE  #                    0                0


------------------ show platform software dtls chassis active F0 statistics ------------------


DTLS Counters     (Success/Failure)
-----------------------------------
Create                  847/0
Delete                  424/0
HW Create               425/0
HW Modify               422/0
HW Delete               424/0
Create Ack              425/0
Modify Ack              422/0
Delete Ack              424/0
Ack Ack Notify          1271/0
Ack Nack Notify         0/0
Nack Notify             0/0
HA Seq GET              782/0
HA Seq SET              0/0
HA Seq Crypto GET       1542/0
HA Seq Crypto SET       0/0
HA Seq Crypto Callback  1542/0

HA Seq last Responsed   0
HA Seq Pending          0
HA Seq Outstanding cb   0
Total DTLS CTX count    1


------------------ show platform software dtls chassis active F0 ------------------


Forwarding Manager DTLS Session Summary

Session ID          Type        Peer IP          Port   AOM ID      Status

------------------------------------------------------------------------------------------

0x0300000000000001  AP Control  78.1.50.1        52345  3270        Done




------------------ show platform hardware chassis active qfp feature wireless dtls cpp-client
 statistics ------------------


DTLS cpp-client plumbing statistics
Number Msg in = ack + nak + ack fail + nak fail + errors

Counter                                        Value
-------------------------------------------------------------------
Create from fp                                 425
Modify from fp                                 422
Delete from fp                                 424
```

```
Create ack to fp                               425
Create ack fail to fp                          0
Create nack to fp                              0
Create nack fail to fp                         0
Modify ack to fp                               422
Modify ack fail to fp                          0
Modify nack to fp                              0
Modify nack fail to fp                         0
Delete ack to fp                               424
Delete ack fail to fp                          0
Delete nack to fp                              0
Delete nak fail to fp                          0


------------------ show platform hardware chassis active qfp feature wireless dtls cpp-client
 summary ------------------

    Session ID          CDH Handle      Session Type     Parent if-h        Instance id

-----------------------------------------------------------------------------------------

0x0300000000000001  0x00000000D902D9E0   AP Control           0                  3



------------------ show platform hardware chassis active qfp feature wireless dtls datapath
 summary ------------------


Src IP          Dst IP          Src Port Dst Port   Crypto HDL         Instance Id
------          ------          -------- -------    -----------        ----------
78.1.1.7        78.1.50.1       5246     52345      0xd902d9e0           3

------------------ show platform hardware chassis active qfp feature wireless dtls datapath
 statistics ------------------


CPP Wireless DTLS Feature Stats

                             Description     Packet Count      Octet Count
                             -----------     ------------      -----------
   DTLS Packets To Encrypt                         286494          8860778
   DTLS Packets Encrypted                          286494         35681366
   DTLS Packets To Decrypt                         286734         41001830
   DTLS Packets Decrypted                          286734         33401602
   Skip Encryption - Handshake                          0                0
   Skip Encryption - Not AppData                        0                0
   Skip Encryption - No Hash Entry                      0                0
   Skip Encryption - No Crypto Handle                   0                0
   Skip Encryption - No DTLS header                   563            76419
   Skip Encryption - Requested by RP                16234          5042852
   Skip Decryption - Handshake                          0                0
   Skip Decryption - Not AppData                     2949           996248
   Skip Decryption - No Hash Entry                    447            56474
   Skip Decryption - No Crypto Handle               13024          3626640
   Skip Decryption - No DTLS header                   507           116600
   Skip Decryption - Multiple Records                   0                0
   Error - Encrypt Invalid Length                       0                0
   Error - Encrypt Header Restore                       0                0
   Error - DataEncrypt No Crypto Handle                 0                0
   Error - DataEncrypt Header Restore                   0                0
   Error - Decrypt Invalid Length                       0                0
   Error - Decrypt Header Restore                       0                0
   Error - DataDecrypt Zero Epoch                       0                0
   Error - DataDecrypt No Hash Entry                  0                0
   Error - DataDecrypt No Crypto Handle               0                0
   Error - DataDecrypt Header Restore                 0                0


------------------ show platform software wireless-client chassis active F0 statistics
------------------


Client Counters   (Success/Failure)
-----------------------------------
Create                 112/0
Delete                 55/0
HW Create              56/0
HW Modify              56/0
HW Delete              55/0
Create Ack             56/0
Modify Ack             56/0
Delete Ack             55/0
NACK Notify            0/0


------------------ show platform software wireless-client chassis active F0 ------------------



        ID  MAC Address     WLAN  Client State           AOM ID  Status
-----------------------------------------------------------------------------
0xa0000001  0028.b122.0001     1  Run                      3272  Done




------------------ show platform hardware chassis active qfp feature wireless wlclient
cpp-client statistics ------------------


Wlclient cpp-client plumbing statistics
Number Msg in = ack + nak + ack fail + nak fail + errors

Counter                                        Value
-------------------------------------------------------------------
Create from fp                                 56
Modify from fp                                 56
Delete from fp                                 55
Create ack to fp                               56
Create ack fail to fp                          0
Create nack to fp                              0
Create nack fail to fp                         0
Modify ack to fp                               56
Modify ack fail to fp                          0
Modify nack to fp                              0
Modify nack fail to fp                         0
Delete ack to fp                               55
Delete ack fail to fp                          0
Delete nack to fp                              0
Delete nak fail to fp                          0


------------------ show platform hardware chassis active qfp feature wireless wlclient
cpp-client summary ------------------

Auth State Abbreviations:
  UK - UNKNOWN IP - LEARN IP
  L3 - L3 AUTH RN - RUN
  IV - INVALID
Mobility State Abbreviations:
  UK - UNKNOWN IN - INIT
  LC - LOCAL   AN - ANCHOR
  FR - FOREIGN MT - MTE
  IV - INVALID
 CPP IF_H     DPIDX      MAC Address    VLAN  AS  MS                WLAN
  POA
------------------------------------------------------------------------------------------

  0X102     0XA0000001  0028.b122.0001  177   RN  LC                 att
0x90000042


------------------ show platform hardware chassis active qfp feature wireless wlclient
datapath summary ------------------


Vlan   pal_if_hdl   mac            Input Uidb Output Uidb
------ ------------ -------------- ---------- -----------
177    0xa0000001   0028.b122.0001 95744      95742


------------------ show platform hardware chassis active qfp feature wireless wlclient
datapath statistic drop ------------------



Drop Cause                                                                Packets
      Octets
============================================================ ====================
====================
Wls Client V6 Max Address Error                                                 0
           0
Wls Client IPGlean Counter Index Error                                          0
           0
Wls Client IPGlean Counter Unchanged Error                                      0
           0
Wls Client IPGlean alloc no memory Error                                        0
           0
Wls Client invalid punt packet error                                            0
           0
Wls Client input subblock missing error                                         0
           0
Wls Client input config missing                                                 0
           0
Wls Client global mac address fetch error                                       0
           0
Wls Client header add error                                                     0
           0
Wls Client IP entry theft error                                                 0
           0
Wls Client IPSG input subblock missing error                                    0
           0
Wls Client DOT1Q Hdr add anchor error                                           0
           0
Wls Client DOT1Q Hdr add anchor avc error                                       0
           0
Wls Client Guest Foreign Multicast error                                        0
           0


------------------ show platform hardware chassis active qfp feature wireless wlclient
datapath table dataglean all ------------------
```

```
CPP Wireless IPv6 Data Gleaning Table:

IP Address                                VLAN    uIDB   Interface
----------------------------------------  ----  ------  -------------


------------------ show platform hardware chassis active qfp feature wireless ipsg cpp-client
 statistics ------------------

CPP Wireless IPSG CPP-client Statistics
Counter                         Value
----------------------------------------------------
Total IPv4 Address Count        1
Total IPv6 Address Count        0
IPv4 Entry Add Success          56
IPv4 Entry Add Fail             0
IPv4 Entry Delete Success       55
IPv4 Entry Delete Fail          0
IPv6 Entry Add Success          0
IPv6 Entry Add Fail             0
IPv6 Entry Delete Success       0
IPv6 Entry Delete Fail          0
IP Entry Override               0
IP Entry Add Req Skip           0
Data Glean Memory Req Recv      0
Data Glean Memory Req Fail      0
Data Glean Memory Reg Send      0
Data Glean Memory Ret Recv      0
Data Glean Memory Ret Send      0
Data Glean Entry Send           0
IPSG Subblock Allocate          0
IPSG Subblock Allocate Fail     0
IPSG Subblock Free              0
IPSG Subblock Free Fail         0
IPSG FIA Enable                 0
IPSG FIA Enable Fail            0
IPSG FIA Disable                0
IPSG FIA Disable Fail           0
IPSG Feature Enable             0
IPSG Feature Enable Fail        0
IPSG Feature Disable            0
IPSG Feature Disable Fail       0


------------------ show platform hardware chassis active qfp feature wireless ipsg cpp-client
 table ipv4 all ------------------

CPP Wireless IPSG Table Summary
Total number of address entries: 1
IP Address                                VLAN  uIDB
-----------------------------------------------------
177.1.0.7                                 177   95744


------------------ show platform hardware chassis active qfp feature wireless ipsg cpp-client
 table ipv6 all ------------------

CPP Wireless IPSG Table Summary
Total number of address entries: 0


------------------ show platform hardware chassis active qfp feature wireless ipsg datapath
```

```
 statistics global ------------------


  Wireless IPSG Global Statistics
  ---------------------------------
    IPv6 Dataglean entry add          :  0
    IPv6 Dataglean entry remove       :  0
    IPv6 Dataglean allocation fail    :  0
    IPv6 Dataglean pool req send      :  0
    IPv6 Dataglean pool req send fail :  0
    IPv6 Dataglean pool req resp      :  0
    IPv6 Dataglean pool ret send      :  0
    IPv6 Dataglean pool ret send fail :  0
    IPv6 Dataglean punt packet        :  0
    IPv6 Dataglean drop packet        :  0


------------------ show platform hardware chassis active qfp feature wireless ipsg datapath
 table ipv4 all ------------------


CPP Wireless IPSG IPv4 Table:

IP Address                                VLAN    uIDB   Interface
----------------------------------------  ----  ------  -------------
177.1.0.7                                  177   95744  WLCLIENT-IF-0x00a0000001


------------------ show platform hardware chassis active qfp feature wireless ipsg datapath
 table ipv6 all ------------------


CPP Wireless IPSG IPv6 Table:

IP Address                                VLAN    uIDB   Interface
----------------------------------------  ----  ------  -------------


------------------ show platform hardware chassis active qfp feature wireless halo statistics
 ------------------


Wireless HALO Statistics
                         Rx Packet Count                0
                         Rx Packet Bytes                0


------------------ show platform hardware chassis active qfp feature wireless fqdn-filter
summary ------------------


CPP Wireless FQDN Filter Info:
ID   Type     DSA_hdl    Redirect_IPv4    Virtual_IPv4
---- -------- ---------- ---------------- ----------------


------------------ show platform hardware chassis active qfp feature wireless et-analytics
 statistics ------------------


Wireless ETA cpp-client plumbing statistics
Number of ETA pending clients : 0

Counter                                         Value
```

```
--------------------------------------------------------------------
Enable ETA on wireless client called           0
Delete ETA on wireless client called           0
ETA global cfg init cb TVI FIA enable error    0
ETA global cfg init cb output SB read error    0
ETA global cfg init cb output SB write error   0
ETA global cfg init cb input SB read error     0
ETA global cfg init cb input SB write error    0
ETA global cfg init cb TVI FIA enable success  0
ETA global cfg uninit cb ingress feat disable  0
ETA global cfg uninit cb ingress cfg delete e  0
ETA global cfg uninit cb egress feat disable   0
ETA global cfg uninit cb egress cfg delete er  0
ETA pending list insert entry called           0
ETA pending list insert invalid arg error      0
ETA pending list insert entry exists error     0
ETA pending list insert no memory error        0
ETA pending list insert entry failed           0
ETA pending list insert entry success          0
ETA pending list delete entry called           0
ETA pending list delete invalid arg error      0
ETA pending list delete entry missing          0
ETA pending list delete entry remove error     0
ETA pending list delete entry success          0


------------------ show platform hardware chassis active qfp feature wireless et-analytics
 eta-pending-client-tree ------------------
```

# show tech-support wireless fabric

To display global fabric parameters, use the **show tech-support wireless fabric** command in privileged EXEC mode.

**show tech-support wireless fabric**

## Syntax Description

This command has no keywords or arguments.

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

The output of the following commands are displayed as part of **show tech-support wireless fabric** command:

- show wireless fabric summary
- show wireless profile fabric summary
- show fabric wlan summary
- show fabric ap summary
- show wireless fabric client summary
- show wireless fabric media-stream client summary
- show wireless stats fabric memory
- show wireless stats fabric control-plane all

### Example

The following is sample output from the **show tech-support wireless fabric** command

# show tech-support wireless mobility

To print the data related to mobility, use the **show tech-support wireless mobility** command in privileged EXEC mode.

**show tech-support wireless mobility**

### Syntax Description

This command has no keywords or arguments.

### Command Default

None

### Command Modes

Privileged EXEC (#)

### Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

### Usage Guidelines

The output of the following commands are displayed as part of **show tech-support wireless mobility** command:

- show platform hardware chassis active qfp feature wireless capwap cpp-client summary
- show platform hardware chassis active qfp feature wireless capwap datapath summary
- show platform hardware chassis active qfp feature wireless dtls cpp-client summary
- show platform hardware chassis active qfp feature wireless dtls datapath statistics
- show platform hardware chassis active qfp feature wireless dtls datapath summary
- show platform software capwap chassis active f0
- show platform software capwap chassis active r0
- show platform software dtls chassis active f0
- show platform software dtls chassis active r0
- show platform software ipc queue-based mobilityd chassis active R0 connection
- show platform software memory messaging mobilityd chassis active R0
- show platform software memory mobilityd chassis active R0 brief
- show wireless mobility ap-list
- show wireless mobility summary
- show wireless stats mobility
- show wireless stats mobility messages

In the presence of standby node, the output of the following mobility commands are also be displayed:

- show platform hardware chassis standby qfp feature wireless capwap cpp-client summary

- show platform hardware chassis standby qfp feature wireless capwap datapath summary
- show platform hardware chassis standby qfp feature wireless dtls cpp-client summary
- show platform hardware chassis standby qfp feature wireless dtls datapath statistics
- show platform hardware chassis standby qfp feature wireless dtls datapath summary
- show platform software capwap chassis standby f0
- show platform software capwap chassis standby r0
- show platform software dtls chassis standby f0
- show platform software dtls chassis standby r0
- show platform software ipc queue-based mobilityd chassis standby R0 connection
- show platform software memory messaging mobilityd chassis standby R0
- show platform software memory mobilityd chassis standby R0 brief
- show wireless stats mobility messages chassis standby r0

### Example

The following is sample output from the **show tech-support wireless mobility** command

```
Device# show tech-support wireless mobility

------------------ show wireless stats mobility ------------------



Mobility event statistics:
     Joined as
         Local                         : 0
         Foreign                       : 0
         Export foreign                : 0
         Export anchor                 : 0
     Delete
         Local                         : 0
         Remote                        : 0
     Role changes
         Local to anchor               : 0
         Anchor to local               : 0
     Roam stats
         L2 roam count                 : 0
         L3 roam count                 : 0
         Flex client roam count        : 0
         Inter-WNCd roam count         : 0
         Intra-WNCd roam count         : 0
     Anchor Request
         Sent                          : 0
           Grant received              : 0
           Deny received               : 0
         Received                      : 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            :
            Ok                       : 0
            Deny - generic           : 0
            Client blacklisted       : 0
            Client limit reached     : 0
            Profile mismatch         : 0
            Deny - unknown reason    : 0
        Request Received             : 0
        Response Sent                :
            Ok                       : 0
            Deny - generic           : 0
            Client blacklisted       : 0
            Client limit reached     : 0
            Profile mismatch         : 0
MM mobility event statistics:
     Event data allocs               : 0
     Event data frees                : 0
     FSM set allocs                  : 0
     FSM set frees                   : 0
     Timer allocs                    : 0
     Timer frees                     : 0
     Timer starts                    : 0
     Timer stops                     : 0
     Invalid events                  : 0
     Internal errors                 : 0


MMIF mobility event statistics:
     Event data allocs               : 0
     Event data frees                : 0
     Invalid events                  : 0
     Unkown events                   : 0
     Event schedule errors           : 0
     Internal errors                 : 0



------------------- show wireless stats mobility messages -------------------



MM datagram message statistics:
  Message Type               Built  Tx    Rx    Processed  Tx Error  Rx Error  Forwarded
Retry  Drops  Allocs  Frees

------------------------------------------------------------------------------------------

  Mobile Announce            0      0     0     0          0         0         0
0      0      0       0
  Mobile Announce Nak        0      0     0     0          0         0         0
0      0      0       0
```

```
  Static IP Mobile Annc      0      0     0     0          0         0         0
0      0      0       0
  Static IP Mobile Annc Rsp  0      0     0     0          0         0         0
0      0      0       0
  Handoff                    0      0     0     0          0         0         0
0      0      0       0
  Handoff End                0      0     0     0          0         0         0
0      0      0       0
  Handoff End Ack            0      0     0     0          0         0         0
0      0      0       0
  Anchor Req                 0      0     0     0          0         0         0
0      0      0       0
  Anchor Grant               0      0     0     0          0         0         0
0      0      0       0
  Anchor Xfer                0      0     0     0          0         0         0
0      0      0       0
  Anchor Xfer Ack            0      0     0     0          0         0         0
0      0      0       0
  Export Anchor Req          0      0     0     0          0         0         0
0      0      0       0
  Export Anchor Rsp          0      0     0     0          0         0         0
0      0      0       0
  AAA Handoff                0      0     0     0          0         0         0
0      0      0       0
  AAA Handoff Ack            0      0     0     0          0         0         0
0      0      0       0
  IPv4 Addr Update           0      0     0     0          0         0         0
0      0      0       0
  IPv4 Addr Update Ack       0      0     0     0          0         0         0
0      0      0       0
  IPv6 ND Packet             0      0     0     0          0         0         0
0      0      0       0
  IPv6 Addr Update           0      0     0     0          0         0         0
0      0      0       0
  IPv6 Addr Update Ack       0      0     0     0          0         0         0
0      0      0       0
  Client Add                 0      0     0     0          0         0         0
0      0      0       0
  Client Delete              0      0     0     0          0         0         0
0      0      0       0
  Keepalive Ctrl Req         0      0     0     0          0         0         0
0      0      0       0
  Keepalive Ctrl Resp        0      0     0     0          0         0         0
0      0      0       0
  AP List Update             0      0     0     0          0         0         0
0      0      0       0
  Client Device Profile Info 0      0     0     0          0         0         0
0      0      0       0
  PMK Update                 0      0     0     0          0         0         0
0      0      0       0
  PMK Delete                 0      0     0     0          0         0         0
0      0      0       0
  PMK 11r Nonce Update       0      0     0     0          0         0         0
0      0      0       0
  Device cache Update        0      0     0     0          0         0         0
0      0      0       0
  HA SSO Announce            0      0     0     0          0         0         0
0      0      0       0
  HA SSO Announce Resp       0      0     0     0          0         0         0
0      0      0       0

MM IPC message statistics:
  Message Type               Built  Tx    Rx    Processed  Tx Error  Rx Error  Forwarded
Drops  Allocs  Frees
```

```
------------------------------------------------------------------------------------------

  Mobile Announce            0      0     0     0          0         0         0
0      0       0
  Mobile Announce Nak        0      0     0     0          0         0         0
0      0       0
  Static IP Mobile Annc      0      0     0     0          0         0         0
0      0       0
  Static IP Mobile Annc Rsp  0      0     0     0          0         0         0
0      0       0
  Handoff                    0      0     0     0          0         0         0
0      0       0
  Handoff End                0      0     0     0          0         0         0
0      0       0
  Handoff End Ack            0      0     0     0          0         0         0
0      0       0
  Anchor Req                 0      0     0     0          0         0         0
0      0       0
  Anchor Grant               0      0     0     0          0         0         0
0      0       0
  Anchor Xfer                0      0     0     0          0         0         0
0      0       0
  Anchor Xfer Ack            0      0     0     0          0         0         0
0      0       0
  Export Anchor Req          0      0     0     0          0         0         0
0      0       0
  Export Anchor Rsp          0      0     0     0          0         0         0
0      0       0
  AAA Handoff                0      0     0     0          0         0         0
0      0       0
  AAA Handoff Ack            0      0     0     0          0         0         0
0      0       0
  IPv4 Addr Update           0      0     0     0          0         0         0
0      0       0
  IPv4 Addr Update Ack       0      0     0     0          0         0         0
0      0       0
  IPv6 ND Packet             0      0     0     0          0         0         0
0      0       0
  IPv6 Addr Update           0      0     0     0          0         0         0
0      0       0
  IPv6 Addr Update Ack       0      0     0     0          0         0         0
0      0       0
  Client Add                 0      0     0     0          0         0         0
0      0       0
  Client Delete              0      0     0     0          0         0         0
0      0       0
  Keepalive Ctrl Req         0      0     0     0          0         0         0
0      0       0
  Keepalive Ctrl Resp        0      0     0     0          0         0         0
0      0       0
  AP List Update             0      0     0     0          0         0         0
0      0       0
  Client Device Profile Info 0      0     0     0          0         0         0
0      0       0
  PMK Update                 0      0     0     0          0         0         0
0      0       0
  PMK Delete                 0      0     0     0          0         0         0
0      0       0
  PMK 11r Nonce Update       0      0     0     0          0         0         0
0      0       0
  Device cache Update        0      0     0     0          0         0         0
0      0       0
  HA SSO Announce            0      0     0     0          0         0         0
```

```
0      0       0
  HA SSO Announce Resp       0      0     0     0          0         0         0
0      0       0

MMIF IPC message statistics:
  Message Type              Built  Tx    Rx    Processed  Tx Error  Rx Error  Drops  Allocs
  Frees

------------------------------------------------------------------------------------------

  Mobile Announce            0      0     0     0          0         0         0      0
    0
  Mobile Announce Nak        0      0     0     0          0         0         0      0
    0
  Static IP Mobile Annc      0      0     0     0          0         0         0      0
    0
  Static IP Mobile Annc Rsp  0      0     0     0          0         0         0      0
    0
  Handoff                    0      0     0     0          0         0         0      0
    0
  Handoff End                0      0     0     0          0         0         0      0
    0
  Handoff End Ack            0      0     0     0          0         0         0      0
    0
  Anchor Req                 0      0     0     0          0         0         0      0
    0
  Anchor Grant               0      0     0     0          0         0         0      0
    0
  Anchor Xfer                0      0     0     0          0         0         0      0
    0
  Anchor Xfer Ack            0      0     0     0          0         0         0      0
    0
  Export Anchor Req          0      0     0     0          0         0         0      0
    0
  Export Anchor Rsp          0      0     0     0          0         0         0      0
    0
  AAA Handoff                0      0     0     0          0         0         0      0
    0
  AAA Handoff Ack            0      0     0     0          0         0         0      0
    0
  IPv4 Addr Update           0      0     0     0          0         0         0      0
    0
  IPv4 Addr Update Ack       0      0     0     0          0         0         0      0
    0
  IPv6 ND Packet             0      0     0     0          0         0         0      0
    0
  IPv6 Addr Update           0      0     0     0          0         0         0      0
    0
  IPv6 Addr Update Ack       0      0     0     0          0         0         0      0
    0
  Client Add                 0      0     0     0          0         0         0      0
    0
  Client Delete              0      0     0     0          0         0         0      0
    0
  Keepalive Ctrl Req         0      0     0     0          0         0         0      0
    0
  Keepalive Ctrl Resp        0      0     0     0          0         0         0      0
    0
  AP List Update             0      0     0     0          0         0         0      0
    0
  Client Device Profile Info 0      0     0     0          0         0         0      0
    0
  PMK Update                 0      0     0     0          0         0         0      0
    0
  PMK Delete                0      0     0     0          0         0         0      0
    0
  PMK 11r Nonce Update      0      0     0     0          0         0         0      0
    0
  Device cache Update       0      0     0     0          0         0         0      0
    0
  HA SSO Announce           0      0     0     0          0         0         0      0
    0
  HA SSO Announce Resp      0      0     0     0          0         0         0      0
    0


------------------ show wireless mobility summary ------------------


Mobility Summary

Wireless Management VLAN: 32
Wireless Management IP Address: 9.12.32.10
Mobility Control Message DSCP Value: 48
Mobility Keepalive Interval/Count: 10/3
Mobility Group Name: default
Mobility Multicast Ipv4 address: 0.0.0.0
Mobility Multicast Ipv6 address: ::
Mobility MAC Address: 001e.f6c1.f6ff

Controllers configured in the Mobility Domain:

 IP               Public Ip         Group Name                      Multicast IPv4
Multicast IPv6                                Status                        PMTU
------------------------------------------------------------------------------------------
9.12.32.10        N/A               default                         0.0.0.0           ::
                                           N/A                         N/A


------------------ show wireless mobility ap-list ------------------



------------------ show platform software capwap chassis active r0 ------------------



------------------ show platform software capwap chassis active f0 ------------------



------------------ show platform software dtls chassis active r0 ------------------



------------------ show platform software dtls chassis active f0 ------------------



------------------ show platform hardware chassis active qfp feature wireless capwap
cpp-client summary ------------------



------------------ show platform hardware chassis active qfp feature wireless dtls cpp-client
 summary ------------------
```

```
------------------ show platform hardware chassis active qfp feature wireless capwap datapath
 summary ------------------


Vrf Src Port Dst IP          Dsp Port Input Uidb Output Uidb Instance Id
--- -------- ------          -------- ---------- ----------- -----------


------------------ show platform hardware chassis active qfp feature wireless dtls datapath
 statistics ------------------


CPP Wireless DTLS Feature Stats

                             Description     Packet Count      Octet Count
                             -----------     ------------      -----------
   DTLS Packets To Encrypt                              0                0
   DTLS Packets Encrypted                               0                0
   DTLS Packets To Decrypt                              0                0
   DTLS Packets Decrypted                               0                0
   Skip Encryption - Handshake                          0                0
   Skip Encryption - Not AppData                        0                0
   Skip Encryption - No Hash Entry                      0                0
   Skip Encryption - No Crypto Handle                   0                0
   Skip Encryption - No DTLS header                     0                0
   Skip Encryption - Requested by RP                    0                0
   Skip Decryption - Handshake                          0                0
   Skip Decryption - Not AppData                        0                0
   Skip Decryption - No Hash Entry                      0                0
   Skip Decryption - No Crypto Handle                   0                0
   Skip Decryption - No DTLS header                     0                0
   Skip Decryption - Multiple Records                   0                0
   Error - Encrypt Invalid Length                       0                0
   Error - Encrypt Header Restore                       0                0
   Error - DataEncrypt No Crypto Handle                 0                0
   Error - DataEncrypt Header Restore                   0                0
   Error - Decrypt Invalid Length                       0                0
   Error - Decrypt Header Restore                       0                0
   Error - DataDecrypt Zero Epoch                       0                0
   Error - DataDecrypt No Hash Entry                    0                0
   Error - DataDecrypt No Crypto Handle                 0                0
   Error - DataDecrypt Header Restore                   0                0


------------------ show platform hardware chassis active qfp feature wireless dtls datapath
 summary ------------------


Src IP          Dst IP          Src Port Dst Port   Crypto HDL         Instance Id
------          ------          -------- -------    -----------        ----------

------------------ show platform software ipc queue-based mobilityd chassis active R0
connection ------------------

Name: -mobilityd_to_wncd-b0
  Number     : 0
  Mode       : writer
  Created on : 03/22/18 05:35:06
  Queue Size : 524288 bytes, 0 bytes currently used
  Enqueued   : 12 msgs, 432 bytes, 0 err, 0 back-pressures,
               360 bytes max queue utilization,
               0 times reached above 90%, 0 times reached above 75%
```

```
Name: -mobilityd_to_wncd-b1
  Number     : 1
  Mode       : writer
  Created on : 03/22/18 05:35:06
  Queue Size : 524288 bytes, 0 bytes currently used
  Enqueued   : 12 msgs, 432 bytes, 0 err, 0 back-pressures,
               360 bytes max queue utilization,
               0 times reached above 90%, 0 times reached above 75%

Name: -mobilityd_to_wncd-b2
  Number     : 2
  Mode       : writer
  Created on : 03/22/18 05:35:06
  Queue Size : 524288 bytes, 0 bytes currently used
  Enqueued   : 12 msgs, 432 bytes, 0 err, 0 back-pressures,
               360 bytes max queue utilization,
               0 times reached above 90%, 0 times reached above 75%

Name: -mobilityd_to_fman_rp-b0
  Number     : 3
  Mode       : writer
  Created on : 03/22/18 05:35:06
  Queue Size : 524288 bytes, 0 bytes currently used
  Enqueued   : 0 msgs, 0 bytes, 0 err, 0 back-pressures,
               0 bytes max queue utilization,
               0 times reached above 90%, 0 times reached above 75%

Name: -mobilityd_to_iosd_rp-b0
  Number     : 4
  Mode       : writer
  Created on : 03/22/18 05:35:06
  Queue Size : 524288 bytes, 0 bytes currently used
  Enqueued   : 204647 msgs, 15757819 bytes, 0 err, 0 back-pressures,
               81 bytes max queue utilization,
               0 times reached above 90%, 0 times reached above 75%

Name: -mobilityd_to_wncmgrd-b0
  Number     : 5
  Mode       : writer
  Created on : 03/22/18 05:35:06
  Queue Size : 524288 bytes, 0 bytes currently used
  Enqueued   : 12 msgs, 432 bytes, 0 err, 0 back-pressures,
               360 bytes max queue utilization,
               0 times reached above 90%, 0 times reached above 75%

Name: -odm_clnt2svr_data-mobilityd-000-1
  Number     : 6
  Mode       : writer
  Created on : 03/22/18 05:35:06
  Queue Size : 2097152 bytes, 0 bytes currently used
  Enqueued   : 33 msgs, 12535 bytes, 0 err, 0 back-pressures,
               3769 bytes max queue utilization,
               0 times reached above 90%, 0 times reached above 75%

Name: -odm_svr2clnt_data-mobilityd-000-1
  Number     : 7
  Mode       : reader
  Created on : 03/22/18 05:35:06
  Queue Size : 2097152 bytes, 0 bytes currently used
  Dequeued   : 0 msgs, 0 bytes, 0 err

Name: -fman_rp_to_mobilityd-b0
  Number     : 8
  Mode       : reader
  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
```

```
[tdl_sr] type repl_database_name/e9118a691a20b4b8f1118bc37a894603/0 created:33 destroyed:33
 diff:0
[tdl_sr] type repl_pkey_tdl/83de2d20ec3ca19b8ae9a89147480a25/1 created:33 destroyed:33
diff:0
[tdl_sr] type repl_blob_tdl/016a67083ea407334130436c855ae237/0 created:33 destroyed:33
diff:0
[tdl_sr] type repl_luid/b9c9d9f4876af528cb82273df98479d6/0 created:33 destroyed:33 diff:0
[tdl_sr] type repl_objinfo/6c8800fedf8d71512f9b6c9754db3a70/0 created:33 destroyed:33 diff:0
[tdl_sr] message repl_trec_update/15fe2a39409473179c9e7111851b2196/0 created:33 destroyed:33
 diff:0
[pki_ssl] type buff/941d8a519d6f23d27067617119f1bb38/0 created:613944 destroyed:613944
diff:0
[pki_ssl] type get_certid_params/0d7bcce690f74649c2e33bbf341e2229/0 created:204648
destroyed:204648 diff:0
[pki_ssl] type get_certid_callback_params/708b7fb964ace7971d90a452c830488c/0 created:204648
 destroyed:204648 diff:0
[pki_ssl] message get_certid/ee3bfe6b93901440346417a4ad67fa63/0 created:204648
destroyed:204648 diff:0
[pki_ssl] message get_certid_callback/372218059d7a753ba73f7b06f18532e9/0 created:204648
destroyed:204648 diff:0
[svc_defs] type svc_loc/929237802cf26e862f8e8716169e31ef/0 created:40952 destroyed:40951
diff:1
[ui_shr] type ui_client/bec7457db0c33cae9eeebbf80073b771/0 created:3 destroyed:2 diff:1
[ui] type ui_info/4b8b42a883fabbb98ec8b919f60e4ad6/0 created:40949 destroyed:40949 diff:0
[ui] type ui_req/69f1e2a5943e050f0aa12df8639ba442/0 created:3 destroyed:2 diff:1
[ui] type event_statistics/7f346ee47165c035a72e139b84afb2a0/0 created:40948 destroyed:40948
 diff:0
[ui] type hostinfo_data/54d5a8b0cd4d29d575b2fc0d91695b5e/0 created:3 destroyed:3 diff:0
[ui] message ui_info_msg/bec533dd713e0222cb8fe5df868031f0/0 created:1 destroyed:1 diff:0
[ui] message ui_req_msg/ac9905cc4488c976847affab56d8b50c/0 created:3 destroyed:2 diff:1
[ui] message process_event_statistics/65d07aa3a04ad950cddd46444df6bc02/0 created:40948
destroyed:40948 diff:0
[ui] message hostinfo_notify/2e9d975712b85b41bc489a6adbc4a46c/0 created:3 destroyed:3 diff:0
[uipeer_comm_ui] type mqipc_enqueue_stats/8f41e408c97a799a5e431d2279acd8de/0 created:8
destroyed:8 diff:0
[uipeer_comm_ui] type mqipc_dequeue_stats/aafe5d0a37ba9652d68550efa26eb0b6/0 created:8
destroyed:8 diff:0
[uipeer_comm_ui] type mqipc_connection_properties/35bd274fd85f7359066f898f25c853ee/0
created:16 destroyed:16 diff:0
[uipeer_comm_ui] message mqipc_connection/a1b22c74b279335b895531ce708c804b/0 created:16
destroyed:16 diff:0
[mem_stats_ui] type tdl_variant_stat/bd85e4b89fb10501e68c1a3cedb9f321/0 created:1 destroyed:0
 diff:1
[mem_stats_ui] message tdl_mem_stats/60ffd9d51213767d041b543869df15d2/0 created:1 destroyed:0
 diff:1
[cdlcore] type cdl_params/a3e74327d37abf27f799f2b5155f4923/0 created:2 destroyed:1 diff:1
[cdlcore] message cdl_message/35205e535c7ab2cdcb3c265ac788f973/0 created:2 destroyed:1
diff:1
[odm_defs] type odm_context/73aeecb77a1ccb6e44f690745cdafe0d/1 created:23 destroyed:23
diff:0
[odm_defs] type odm_register_info/48a7d590e9df0cc9d150801315c50307/1 created:4 destroyed:4
 diff:0
[odm_defs] type odm_table_register_info/4f355a34615affd49af9f90b679d8ce5/1 created:17
destroyed:17 diff:0
[odm_defs] type odm_register_result/53ba304bc0a71a7d2a044518c21f662a/0 created:2 destroyed:2
 diff:0
[odm_defs] message odm_register/2c98272b43d973fa08bbf5acdf3106b0/0 created:2 destroyed:2
diff:0
[odm_defs] message odm_table_register/46694ec1005c3b084337748eeb3768cd/0 created:17
destroyed:17 diff:0
[odm_defs] message odm_register_done/1f6c8f81fcbb8a3052428bab7588e8b5/0 created:2 destroyed:2
 diff:0
[odm_defs] message odm_register_ack/03b8040ed4f7b03517b410c32568ecaa/0 created:2 destroyed:2
 diff:0
```

```
------------------ show platform software memory mobilityd chassis active R0 brief
------------------

  module                  allocated     requested     allocs        frees
  -------------------------------------------------------------------------------
  Summary                 620441        617113        233           25
  unknown                 198515        198435        5             0
  chunk                   139689        139209        30            0
  eventutil               118939        118299        48            8
  process                 67642         67594         3             0
  odm-db-ctx              29950         28430         100           5
  uipeer                  22672         22592         11            6
  odm-ipc-ctx             20272         19984         18            0
  unknown                 18024         18008         1             0
  odm-client-ctx          1872          1824          3             0
  cdllib                  1688          1672          3             2
  trccfg                  512           496           5             4
  bidb                    472           456           1             0
  unknown                 96            48            3             0
  bcrdu_avl               72            56            1             0
  orchestrator_main       26            10            1             0
```

# show tech-support wireless radio

To print the data related to the radio, use the **show tech-support wireless radio** command in privileged EXEC mode.

**show tech-support wireless radio**

### Syntax Description

This command has no keywords or arguments.

### Command Default

None

### Command Modes

Privileged EXEC (#)

### Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

### Usage Guidelines

The output of the following commands are displayed as part of **show tech-support wireless radio** command:

- show ap auto-rf dot11 24ghz
- show ap auto-rf dot11 5ghz
- show ap config dot11 dual-band summary
- show ap config general
- show ap dot11 24ghz channel
- show ap dot11 24ghz coverage
- show ap dot11 24ghz group
- show ap dot11 24ghz high-density
- show ap dot11 24ghz load-info
- show ap dot11 24ghz monitor
- show ap dot11 24ghz network
- show ap dot11 24ghz summary
- show ap dot11 24ghz txpower
- show ap dot11 5ghz channel
- show ap dot11 5ghz coverage
- show ap dot11 5ghz group
- show ap dot11 5ghz high-density
- show ap dot11 5ghz load-info

- show ap dot11 5ghz monitor
- show ap dot11 5ghz network
- show ap dot11 5ghz summary
- show ap dot11 5ghz txpower
- show ap fra
- show ap rf-profile name 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
```

```
    Minimum                                  : unknown
    Average                                  : unknown
    Maximum                                  : -128 dBm
  Channel Dwell Times
    Minimum                                  : unknown
    Average                                  : unknown
    Maximum                                  : unknown
  802.11b 2.4 GHz Auto-RF Channel List
    Allowed Channel List                     : 1,6,11
    Unused Channel List                      : 2,3,4,5,7,8,9,10


------------------ show ap dot11 5ghz channel ------------------


Leader Automatic Channel Assignment
  Channel Assignment Mode                    : AUTO
  Channel Update Interval                    : 600 seconds
  Anchor time (Hour of the day)              : 0
  Channel Update Contribution
    Noise                                    : Enable
    Interference                             : Enable
    Load                                     : Disable
    Device Aware                             : Disable
  CleanAir Event-driven RRM option           : Disabled
  Channel Assignment Leader                  : ewlc-doc (9.12.32.10)
  Last Run                                   : 552 seconds ago

  DCA Sensitivity Level                      : MEDIUM : 15 dB
  DCA 802.11n/ac Channel Width               : 20 MHz
  DCA Minimum Energy Limit                   : -95 dBm
  Channel Energy Levels
    Minimum                                  : unknown
    Average                                  : unknown
    Maximum                                  : -128 dBm
  Channel Dwell Times
    Minimum                                  : unknown
    Average                                  : unknown
    Maximum                                  : unknown
  802.11a 5 GHz Auto-RF Channel List
    Allowed Channel List                     :
36,40,44,48,52,56,60,64,100,104,108,112,116,120,124,128,132,136,140,144,149,153,157,161
    Unused Channel List                      : 165


------------------ show ap dot11 24ghz coverage ------------------


Coverage Hole Detection
  802.11b Coverage Hole Detection Mode             : Enabled
  802.11b Coverage Voice Packet Count              : 100 packet(s)
  802.11b Coverage Voice Packet Percentage         : 50%
  802.11b Coverage Voice RSSI Threshold            : -80 dBm
  802.11b Coverage Data Packet Count               : 50 packet(s)
  802.11b Coverage Data Packet Percentage          : 50%
  802.11b Coverage Data RSSI Threshold             : -80 dBm
  802.11b Global coverage exception level          : 25 %
  802.11b Global client minimum exception level    : 3 clients


------------------ show ap dot11 5ghz coverage ------------------


Coverage Hole Detection
```

```
  802.11a Coverage Hole Detection Mode          : Enabled
  802.11a Coverage Voice Packet Count           : 100 packet(s)
  802.11a Coverage Voice Packet Percentage      : 50 %
  802.11a Coverage Voice RSSI Threshold         : -80dBm
  802.11a Coverage Data Packet Count            : 50 packet(s)
  802.11a Coverage Data Packet Percentage       : 50 %
  802.11a Coverage Data RSSI Threshold          : -80dBm
  802.11a Global coverage exception level       : 25 %
  802.11a Global client minimum exception level : 3 clients


------------------ show ap dot11 24ghz group ------------------


Radio RF Grouping

  802.11b Group Mode               : AUTO
  802.11b Group Update Interval    : 600 seconds
  802.11b Group Leader             : ewlc-doc (9.12.32.10)
  802.11b Last Run                 : 553 seconds ago


RF Group Members

Controller name                  Controller IP
--------------------------------------------------
ewlc-doc                          9.12.32.10




------------------ show ap dot11 5ghz group ------------------


Radio RF Grouping

  802.11a Group Mode               : AUTO
  802.11a Group Update Interval    : 600 seconds
  802.11a Group Leader             : ewlc-doc (9.12.32.10)
  802.11a Last Run                 : 553 seconds ago


RF Group Members

Controller name                  Controller IP
--------------------------------------------------
ewlc-doc                          9.12.32.10




------------------ show ap dot11 24ghz high-density ------------------



------------------ show ap dot11 5ghz high-density ------------------



------------------ show ap dot11 5ghz load-info ------------------



------------------ show ap dot11 24ghz load-info ------------------
```

```
------------------ show ap dot11 24ghz profile ------------------


Default 802.11b AP performance profiles
  802.11b Global Interference threshold    : 10 %
  802.11b Global noise threshold           : -70 dBm
  802.11b Global RF utilization threshold  : 80 %
  802.11b Global throughput threshold      : 1000000 bps
  802.11b Global clients threshold         : 12 clients


------------------ show ap dot11 5ghz profile ------------------


Default 802.11a AP performance profiles

  802.11a Global Interference threshold          : 10 %
  802.11a Global noise threshold                 : -70 dBm
  802.11a Global RF utilization threshold        : 80 %
  802.11a Global throughput threshold            : 1000000 bps
  802.11a Global clients threshold               : 12 clients


------------------ show ap dot11 24ghz monitor ------------------


Default 802.11b AP monitoring
  802.11b Monitor Mode                  : Enabled
  802.11b Monitor Channels              : Country channels
  802.11b RRM Neighbor Discover Type    : Transparent
  802.11b AP Coverage Interval          : 180 seconds
  802.11b AP Load Interval              : 60 seconds
  802.11b AP Noise Interval             : 180 seconds
  802.11b AP Signal Strength Interval   : 60 seconds
  802.11b NDP RSSI Normalization        : Enabled


------------------ show ap dot11 5ghz monitor ------------------


Default 802.11a AP monitoring
  802.11a Monitor Mode                  : Enabled
  802.11a Monitor Channels              : Country channels
  802.11a RRM Neighbor Discover Type    : Transparent
  802.11a AP Coverage Interval          : 180 seconds
  802.11a AP Load Interval              : 60 seconds
  802.11a AP Noise Interval             : 180 seconds
  802.11a AP Signal Strength Interval   : 60 seconds
  802.11a NDP RSSI Normalization        : Enabled


------------------ show ap dot11 24ghz network ------------------



802.11b Network                            : Enabled
11gSupport                                 : Enabled
11nSupport                                 : Enabled
802.11b/g Operational Rates
  802.11b 1M                               : Mandatory
  802.11b 2M                                : Mandatory
  802.11b 5.5M                              : Mandatory
  802.11b 11M                               : Mandatory
  802.11g 6M                                : Supported
  802.11g 9M                                : Supported
  802.11g 12M                               : Supported
  802.11g 18M                               : Supported
  802.11g 24M                               : Supported
  802.11g 36M                               : Supported
  802.11g 48M                               : Supported
  802.11g 54M                               : Supported
802.11n MCS Settings:
  MCS 0 : Supported
  MCS 1 : Supported
  MCS 2 : Supported
  MCS 3 : Supported
  MCS 4 : Supported
  MCS 5 : Supported
  MCS 6 : Supported
  MCS 7 : Supported
  MCS 8 : Supported
  MCS 9 : Supported
  MCS 10 : Supported
  MCS 11 : Supported
  MCS 12 : Supported
  MCS 13 : Supported
  MCS 14 : Supported
  MCS 15 : Supported
  MCS 16 : Supported
  MCS 17 : Supported
  MCS 18 : Supported
  MCS 19 : Supported
  MCS 20 : Supported
  MCS 21 : Supported
  MCS 22 : Supported
  MCS 23 : Supported
  MCS 24 : Supported
  MCS 25 : Supported
  MCS 26 : Supported
  MCS 27 : Supported
  MCS 28 : Supported
  MCS 29 : Supported
  MCS 30 : Supported
  MCS 31 : Supported
802.11n Status:
  A-MPDU Tx:
    Priority 0                              : Enabled
    Priority 1                              : Disabled
    Priority 2                              : Disabled
    Priority 3                              : Disabled
    Priority 4                              : Enabled
    Priority 5                              : Enabled
    Priority 6                              : Disabled
    Priority 7                              : Disabled
    Aggregation scheduler                   : Enabled
    Realtime timeout                        : 10
  A-MSDU Tx:
    Priority 0                              : Enable
    Priority 1                              : Enable
    Priority 2                              : Enable
    Priority 3                              : Enable
    Priority 4                              : Enable
    Priority 5                              : Enable
    Priority 6                              : Disable
    Priority 7                            : Disable
  Guard Interval                          : Any
  Rifs Rx                                 : Enabled
Beacon Interval                           : 100
CF Pollable mandatory                     : Disabled
CF Poll Request Mandatory                 : Disabled
CFP Period                                : 4
CFP Maximum Duration                      : 60
Default Channel                           : 1
Default Tx Power Level                    : 1
DTPC Status                               : Enabled
Call Admission Limit                      :
G711 CU Quantum                           :
ED Threshold                              : -50
Fragmentation Threshold                   : 2346
RSSI Low Check                           : Disabled
RSSI Threshold                            : -127 dbm
PBCC Mandatory                            : unknown
Pico-Cell-V2 Status                       : unknown
RTS Threshold                             : 2347
Short Preamble Mandatory                  : Enabled
Short Retry Limit                         : 7
Legacy Tx Beamforming setting             : Disabled
Traffic Stream Metrics Status             : Disabled
Expedited BW Request Status               : Disabled
EDCA profile type check                   : default-wmm
Call Admision 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 bandwith sample-size           : 20
Maximum Number of Clients per AP Radio    : 200


------------------ show ap dot11 5ghz network ------------------



802.11a Network                           : Enabled
11nSupport                                : Enabled
  802.11a Low Band                        : Enabled
  802.11a Mid Band                        : Enabled
  802.11a High Band                       : Enabled
802.11a Operational Rates
  802.11a 6M                              : Mandatory
  802.11a 9M                              : Supported
  802.11a 12M                             : Mandatory
  802.11a 18M                             : Supported
  802.11a 24M                             : Mandatory
  802.11a 36M                             : Supported
  802.11a 48M                             : Supported
  802.11a 54M                             : Supported
802.11n MCS Settings:
  MCS 0 : Supported
  MCS 1 : Supported
  MCS 2 : Supported
  MCS 3 : Supported
  MCS 4 : Supported
  MCS 5 : Supported
  MCS 6 : Supported
  MCS 7 : Supported
  MCS 8 : Supported
  MCS 9 : Supported
  MCS 10 : Supported
  MCS 11 : Supported
  MCS 12 : Supported
  MCS 13 : Supported
  MCS 14 : Supported
  MCS 15 : Supported
  MCS 16 : Supported
  MCS 17 : Supported
  MCS 18 : Supported
  MCS 19 : Supported
  MCS 20 : Supported
  MCS 21 : Supported
  MCS 22 : Supported
  MCS 23 : Supported
  MCS 24 : Supported
  MCS 25 : Supported
  MCS 26 : Supported
  MCS 27 : Supported
  MCS 28 : Supported
  MCS 29 : Supported
  MCS 30 : Supported
  MCS 31 : Supported
802.11n Status:
  A-MPDU Tx:
    Priority 0                            : Enabled
    Priority 1                            : Disabled
    Priority 2                            : Disabled
    Priority 3                            : Disabled
    Priority 4                            : Enabled
    Priority 5                            : Enabled
    Priority 6                            : Disabled
    Priority 7                            : Disabled
    Aggregation scheduler                 : Enabled
    Realtime timeout                      : 10
  A-MSDU Tx:
    Priority 0                            : Enable
    Priority 1                            : Enable
    Priority 2                            : Enable
    Priority 3                            : Enable
    Priority 4                            : Enable
    Priority 5                            : Enable
    Priority 6                            : Disable
    Priority 7                            : Disable
  Guard Interval                          : Any
  Rifs Rx                                 : Enabled
802.11ac                                  : Enabled
  Frame burst                             : Automatic
802.11ac MCS Settings:
Beacon Interval                           : 100
CF Pollable mandatory                     : Disabled
CF Poll Request Mandatory                 : Disabled
CFP Period                                : 4
CFP Maximum Duration                      : 60
Default Channel                           : 36
Default Tx Power Level                    : 1
DTPC Status                               : Enabled
Fragmentation Threshold                   : 2346
```

```
RSSI Low Check                           : Disabled
RSSI Threshold                            : -127 dbm
Pico-Cell-V2 Status                       : unknown
TI Threshold                              :
Legacy Tx Beamforming setting             : Disabled
Traffic Stream Metrics Status             : Disabled
Expedited BW Request Status               : Disabled
EDCA profile type check                   : default-wmm
Call Admision 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 bandwith sample-size           : 20
Maximum Number of Clients per AP Radio    : 200


------------------ show ap dot11 24ghz txpower ------------------


Automatic Transmit Power Assignment

Transmit Power Assignment Mode          : AUTO
Transmit Power Update Interval          : 600 seconds
Transmit Power Threshold                : -70 dBm
Transmit Power Neighbor Count           : 3 APs
Min Transmit Power                      : -10 dBm
Max Transmit Power                      : 30 dBm
Update Contribution
    Noise                               : Enable
    Interference                        : Enable
    Load                                : Disable
    Device Aware                        : Disable
Transmit Power Assignment Leader        : ewlc-doc (9.12.32.10)
Last Run                                : 558 seconds ago


------------------ show ap dot11 5ghz txpower ------------------


Automatic Transmit Power Assignment

Transmit Power Assignment Mode          : AUTO
Transmit Power Update Interval          : 600 seconds
Transmit Power Threshold                : -70 dBm
Transmit Power Neighbor Count           : 3 APs
Min Transmit Power                      : -10 dBm
Max Transmit Power                      : 30 dBm
Update Contribution
    Noise                               : Enable
    Interference                        : Enable
    Load                                : Disable
    Device Aware                        : Disable
Transmit Power Assignment Leader        : ewlc-doc (9.12.32.10)
Last Run                                : 558 seconds ago
```

```
------------------ show ap auto-rf dot11 5ghz ------------------



------------------ show ap auto-rf dot11 24ghz ------------------



------------------ show ap config general ------------------




------------------ show ap dot11 5ghz optimized-roaming ------------------

802.11a OptimizedRoaming

  Mode                                    : Disabled
  Reporting Interval                      : 90 seconds
  Rate Threshold                          : Disabled
  Hysteresis                              : 6 db


------------------ show ap rf-profile summary ------------------



Number of RF-profiles: 6

RF Profile Name                  Band     Description                          State
------------------------------------------------------------------------------------
Low_Client_Density_rf_5gh        5 GHz    pre configured Low Client Density rf Up
High_Client_Density_rf_5gh       5 GHz    pre configured High Client Density r Up
Low_Client_Density_rf_24gh       2.4 GHz  pre configured Low Client Density rf Up
High_Client_Density_rf_24gh      2.4 GHz  pre configured High Client Density r Up
Typical_Client_Density_rf_5gh    5 GHz    pre configured Typical Density rfpro Up
Typical_Client_Density_rf_24gh   2.4 GHz  pre configured Typical Client Densit Up


------------------ show ap fra ------------------

FRA State                                               : Disabled
FRA Sensitivity                                         : medium (95%)
FRA Interval                                            : 1 Hour(s)
  Last Run                                              : 2299 seconds ago
  Last Run time                                         : 0 seconds

AP Name              MAC Address       Slot ID  Current-Band      COF %      Suggested Mode
--------------------------------------------------------------------------------------------

COF : Coverage Overlap Factor


------------------ show wireless band-select ------------------


Band Select Probe Response   : per WLAN enabling
Cycle Count                  : 2
Cycle Threshold (millisec)   : 200
Age Out Suppression (sec)    : 20
Age Out Dual Band (sec)      : 60
Client RSSI (dBm)            : -80
Client Mid RSSI (dBm)        : -80
```

```
------------------ show wireless  country  configure ------------------


Configured Country..........................   US - United States
Configured Country Codes
        US  - United States                  802.11a Indoor/ 802.11b Indoor/ 802.11g Indoor


------------------ show wireless tag rf summary ------------------


Number of RF Tags: 1

RF tag name                       Description
------------------------------------------------------------------------
default-rf-tag                    default RF tag


------------------ show ap tag summary ------------------


Number of APs: 0


------------------ show ap status ------------------


------------------ show ap uptime ------------------


Number of APs: 0
```

# show umbrella config

To view the Umbrella configuration details, use the **show umbrella config** command.

**show umbrella config**

## Syntax Description

This command has no arguments.

## Command Default

None

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the Umbrella configuration details:

```
Device# show umbrella config
Umbrella Configuration
========================
   Token: 57CC80106C087FB1B2A7BAB4F2F4373C00247166
   OrganizationID: 1892929
   Local Domain Regex parameter-map name: dns_wl
   DNSCrypt: Enabled
  Public-key: B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79

   UDP Timeout: 2 seconds
   Resolver address:
       1. 208.67.220.220
       2. 208.67.222.222
       3. 2620:119:53::53
       4. 2620:119:35::35
```

# show umbrella deviceid

To view the device registration details, use the **show umbrella deviceid** command.

**show umbrella deviceid**

## Syntax Description

This command has no arguments.

## Command Default

None

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the device registration details:

```
Device# show umbrella deviceid
Device registration details
Profile Name            Tag              Status           Device-id
GigabitEthernet0/0/0    guest          200 SUCCESS     010a470b042a072d
```

# show umbrella deviceid detailed

To view the detailed description for the Umbrella device ID, use the **show umbrella deviceid detailed** command.

**show umbrella deviceid** *detailed*

## Syntax Description

This command has no arguments.

## Command Default

None

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the detailed description for the Umbrella device ID:

```
Device# show umbrella deviceid detailed
Device registration details
 1.GigabitEthernet0/0/0
      Tag              : guest
      Device-id        : 010a470b042a072d
      Description      : Device Id recieved successfully
```

# show umbrella dnscrypt

To view the Umbrella DNScrypt details, use the **show umbrella dnscrypt** command.

**show umbrella dnscrypt**

### Syntax Description

This command has no arguments.

### Command Default

None

### Command Modes

Global configuration

### Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the Umbrella DNScrypt details:

```
Device# show umbrella dnscrypt
DNSCrypt: Enabled
   Public-key: B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79

   Certificate Update Status:
        Last Successfull Attempt: 17:45:57 IST Nov 9 2017
   Certificate Details:
       Certificate Magic     : DNSC
       Major Version         : 0x0001
       Minor Version         : 0x0000
       Query Magic           : 0x713156774457306E
       Serial Number         : 1490391488
       Start  Time           : 1490391488 (03:08:08 IST Mar 25 2017)
       End Time              : 1521927488 (03:08:08 IST Mar 25 2018)
       Server Public Key     :
E7F8:4477:BF89:1434:1ECE:23F0:D6A6:6EB9:4F45:3167:D71F:80BB:4E80:A04F:F180:F778
       Client Secret Key Hash:
F1A5:1993:F729:5416:53B7:94E3:6509:8182:A708:0561:8050:6CE0:DFA1:5C94:6EE4:0010
       Client Public key     :
BC6D:3758:48B6:120B:D2F5:F25B:2979:564D:F52C:5EFA:B0BD:76FE:3CD6:828B:44D2:FF3A
       NM key Hash           :
1FF7:2E1E:EFB9:7987:9CB4:3EF8:A25B:4DAD:10FC:7DF7:6985:6E8E:6E4D:D56A:1C70:B9EB
```

# show vlan

To display the parameters for all configured VLANs or one VLAN (if the VLAN ID or name is specified) on the switch, use the **show vlan** command in user EXEC mode.

**show vlan** [**brief** | **group** | **id** *vlan-id* | **mtu** | **name** *vlan-name* | **remote-span** | **summary**]

## Syntax Description

| | |
|---|---|
| **brief** | (Optional) Displays one line for each VLAN with the VLAN name, status, and its ports. |
| **group** | (Optional) Displays information about VLAN groups. |
| **id** *vlan-id* | (Optional) Displays information about a single VLAN identified by the VLAN ID number. For *vlan-id*, the range is 1 to 4094. |
| **mtu** | (Optional) Displays a list of VLANs and the minimum and maximum transmission unit (MTU) sizes configured on ports in the VLAN.<br>**Note** Traceback occurs in the VLAN CLI parser when Controller-PI does VLAN lookup for each interface. |
| **name** *vlan-name* | (Optional) Displays information about a single VLAN identified by the VLAN name. The VLAN name is an ASCII string from 1 to 32 characters. |
| **remote-span** | (Optional) Displays information about Remote SPAN (RSPAN) VLANs. |
| **summary** | (Optional) Displays VLAN summary information. |

**Note** The **ifindex** keyword is not supported, even though it is visible in the command-line help string.

## Command Default

None

## Command Modes

User EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

In the **show vlan mtu** command output, the MTU_Mismatch column shows whether all the ports in the VLAN have the same MTU. When yes appears in the column, it means that the VLAN has ports with different MTUs, and packets that are switched from a port with a larger MTU to a port with a smaller MTU might be dropped. If the VLAN does not have an SVI, the hyphen (-) symbol appears in the SVI_MTU column. If the MTU-Mismatch column displays yes, the names of the ports with the MinMTU and the MaxMTU appear.

This is an example of output from the **show vlan** command. See the table that follows for descriptions of the fields in the display.

```
Device> show vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi1/0/2, Gi1/0/3, Gi1/0/4
                                                Gi1/0/5, Gi1/0/6, Gi1/0/7
                                                Gi1/0/8, Gi1/0/9, Gi1/0/10
                                                Gi1/0/11, Gi1/0/12, Gi1/0/13
                                                Gi1/0/14, Gi1/0/15, Gi1/0/16
                                                Gi1/0/17, Gi1/0/18, Gi1/0/19
                                                Gi1/0/20, Gi1/0/21, Gi1/0/22
                                                Gi1/0/23, Gi1/0/24, Gi1/0/25
                                                Gi1/0/26, Gi1/0/27, Gi1/0/28
                                                Gi1/0/29, Gi1/0/30, Gi1/0/31
                                                Gi1/0/32, Gi1/0/33, Gi1/0/34
                                                Gi1/0/35, Gi1/0/36, Gi1/0/37
                                                Gi1/0/38, Gi1/0/39, Gi1/0/40
                                                Gi1/0/41, Gi1/0/42, Gi1/0/43
                                                Gi1/0/44, Gi1/0/45, Gi1/0/46
                                                Gi1/0/47, Gi1/0/48
2    VLAN0002                         active
40   vlan-40                          active
300  VLAN0300                         active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
2    enet  100002     1500  -      -      -        -    -        0      0
40   enet  100040     1500  -      -      -        -    -        0      0
300  enet  100300     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0
2000 enet  102000     1500  -      -      -        -    -        0      0
3000 enet  103000     1500  -      -      -        -    -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------
2000,3000

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

*Table 18: show vlan Command Output Fields*

| Field | Description |
|---|---|
| VLAN | VLAN number. |
| Name | Name, if configured, of the VLAN. |
| Status | Status of the VLAN (active or suspend). |
| Ports | Ports that belong to the VLAN. |

| Field | Description |
|---|---|
| Type | Media type of the VLAN. |
| SAID | Security association ID value for the VLAN. |
| MTU | Maximum transmission unit size for the VLAN. |
| Parent | Parent VLAN, if one exists. |
| RingNo | Ring number for the VLAN, if applicable. |
| BrdgNo | Bridge number for the VLAN, if applicable. |
| Stp | Spanning Tree Protocol type used on the VLAN. |
| BrdgMode | Bridging mode for this VLAN—possible values are source-route bridging (SRB) and source-route transparent (SRT); the default is SRB. |
| Trans1 | Translation bridge 1. |
| Trans2 | Translation bridge 2. |
| Remote SPAN VLANs | Identifies any RSPAN VLANs that have been configured. |

This is an example of output from the **show vlan summary** command:

```
Device> show vlan summary
Number of existing VLANs              : 45
 Number of existing VTP VLANs         : 45
 Number of existing extended VLANS    : 0
```

This is an example of output from the **show vlan id** command:

```
Device# show vlan id 2
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
2    VLAN0200                         active    Gi1/0/7, Gi1/0/8
2    VLAN0200                         active    Gi2/0/1, Gi2/0/2

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
2    enet  100002     1500  -      -      -        -    -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------
Disabled
```

# show vlan access-map

To display information about a particular VLAN access map or for all VLAN access maps, use the **show vlan access-map** command in privileged EXEC mode.

**show vlan access-map** [*map-name*]

## Syntax Description

| | |
|---|---|
| *map-name* | (Optional) Name of a specific VLAN access map. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This is an example of output from the **show vlan access-map** command:

```
Device# show vlan access-map
Vlan access-map "vmap4"  10
  Match clauses:
    ip  address: al2
  Action:
    forward
Vlan access-map "vmap4"  20
  Match clauses:
    ip  address: al2
  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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This is an example of output from the **show vlan filter** command:

```
Device# show vlan filter
VLAN Map map_1 is filtering VLANs:
  20-22
```

# show vlan group

To display the VLANs that are mapped to VLAN groups, use the **show vlan group** command in privileged EXEC mode.

**show vlan group** [**group-name** *vlan-group-name* [**user_count**]]

### Syntax Description

| | |
|---|---|
| **group-name** *vlan-group-name* | (Optional) Displays the VLANs mapped to the specified VLAN group. |
| **user_count** | (Optional) Displays the number of users in each VLAN mapped to a specified VLAN group. |

### Command Default

None

### Command Modes

Privileged EXEC

### Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

### Usage Guidelines

The **show vlan group** command displays the existing VLAN groups and lists the VLANs and VLAN ranges that are members of each VLAN group. If you enter the **group-name** keyword, only the members of the specified VLAN group are displayed.

This example shows how to display the members of a specified VLAN group:

# show wireless stats ap history

To verify historical statistics of an AP, use the **show wireless stats ap history** command.

**show wireless stats ap history**

## Syntax Description

This command has no keywords or arguments.

## Command Default

None

## Command Modes

Privileged EXEC#

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Cupertino 17.7.1 | This command was introduced. |

## Examples

This example shows how to verify the statistics of the access point hisory:

```
Device# show wireless stats ap history
AP Name             Radio MAC       Event      Time                   Recent      Disconnect
Reason          Disconnect
                                                                  Disconnect  Reason
               Count
                                                                  Time
------------------------------------------------------------------------------------------
APA023.9FD8.EA22   40ce.24bf.8ca0  Joined     06/26/21 10:11:52  NA           NA
               NA
APA023.9FD8.EA22   40ce.24bf.8ca0  Disjoined  06/26/21 10:05:18  NA           Heart beat
timer expiry    1
APA023.9FD8.EA22   40ce.24bf.8ca0  Joined     06/22/21 17:00:39  NA           NA
               NA
APA023.9FD8.EA22   40ce.24bf.8ca0  Disjoined  06/22/21 16:54:54  NA           Heart beat
timer expiry    1
APA023.9FD8.EA22   40ce.24bf.8ca0  Joined     06/21/21 23:01:17  NA           NA
               NA
APA023.9FD8.EA22   40ce.24bf.8ca0  Disjoined  06/21/21 22:56:21  NA         Image Download
 Success     1
```

# show wireless stat redundancy statistics client-recovery mobilityd

To view the statistics of Mobilityd configuration database, use the **show wireless stat redundancy statistics client-recovery mobilityd** command.

**show wireless stat redundancy statistics client-recovery mobilityd**

## Syntax Description

This command has no keywords or arguments.

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Cupertino 17.7.1 | This command was introduced. |

## Examples

The following example shows how to view the statistics of Mobilityd configuration database:

```
Device# show wireless stat redundancy statistics client-recovery mobilityd

Mobility Client Deletion Reason Statistics
-------------------------------------------
Mobility Incomplete State         : 0
Inconsistency in WNCD & Mobility  : 0
Partial Delete                    : 0
General statistics
--------------------
```

# show wireless stat redundancy statistics client-recovery sisf

To view the statistics for Switch Integrated Security Features (SISF) configuration database, use the **show wireless stat redundancy statistics client-recovery sisf** command.

**show wireless stat redundancy statistics client-recovery sisf**

## Syntax Description

This command has no keywords or arguments.

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Cupertino 17.7.1 | This command was introduced. |

## Examples

The following example shows how to view the statistics for SISF configuration database:

```
Device# show wireless stat redundancy statistics client-recovery sisf
Client SSO statistics for SISF
--------------------------------
Number of recreate attempted post switchover    : 0
Number of recreate succeeded post switchover    : 0
Number of recreate failed because of no mac     : 0
Number of recreate failed because of no ip      : 0
Number of ipv4 entry recreate success           : 0
Number of ipv4 entry recreate failed            : 0
Number of ipv6 entry recreate success           : 0
Number of ipv6 entry recreate failed            : 0
Number of partial delete received               : 0
Number of client purge attempted                : 0
Number of heap and db entry purge success       : 0
Number of purge success for db entry only       : 0
Number of client purge failed                   : 0
Number of garp sent                             : 0
Number of garp failed                           : 0
Number of IP table create callbacks on standby  : 0
Number of IP table modify callbacks on standby  : 0
Number of IP table delete callbacks on standby  : 0
Number of MAC table create callbacks on standby : 0
Number of MAC table modify callbacks on standby : 0
Number of MAC table delete callbacks on standby : 0
```

# show wireless stat redundancy client-recovery wncd

To view the redundancy configuration statistics for all the Wireless Network Control Daemon (WNCd) instances, use the **show wireless stat redundancy client-recovery wncd** command.

**show wireless stat redundancy client-recovery wncd** { *instance-id* | **all** }

## Syntax Description

| | |
|---|---|
| *instance-id* | Instance ID. Valid values range from 0 to 7. |
| **all** | Specifies the statistics for all WNCd instances. |

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Cupertino 17.7.1 | This command was introduced. |

## Examples

The following example shows how to view the redundancy configuration statistics for all the WNCd instances:

```
Device# show wireless stat redundancy statistics client-recovery wncd all

Client SSO statistics
----------------------
No. of Clients                             : 0
No. of Clients recovered successfully      : 0
No. of Clients failed to recover           : 0
No. of Reconcile messages received from AP : 0
WNCD instance  : 0
Reconcile messages received from AP                     : 0
Reconcile clients received from AP                      : 0
Recreate attempted post switchover                      : 0
Recreate attempted by SANET                             : 0
Recreate attempted by DOT1x                             : 0
Recreate attempted by SISF                              : 0
Recreate attempted by SVC CO                            : 0
Recreate attempted by Unknown module                    : 0
Recreate succeeded post switchover                      : 0
Recreate Failed post switchover                         : 0
Recreate Failure in mmif                                : 0
Recreate Failure in co                                  : 0
Recreate Failure in sanet                               : 0
Recreate Failure in authmgr                             : 0
Recreate Failure in dot1x                               : 0
Recreate Failure in mab                                 : 0
Recreate Failure in sanet_accounting                    : 0
Recreate Failure in sisf                                : 0
Recreate Failure in web auth                            : 0
Recreate Failure in lisp                                :
Recreate Failure in ipv6                                : 0
Recreate Failure in qos                                 : 0
```

# show wireless band-select

To display the status of the band-select configuration, use the **show wireless band-select** command in privileged EXEC mode.

**show wireless band-select**

## Syntax Description

This command has no arguments or keywords.

## Command Default

No default behavior or values.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

The following is sample output from the **show wireless band-select** command:

```
Device# show wireless band-select
Band Select Probe Response    : per WLAN enabling
Cycle Count                  : 2
Cycle Threshold (millisec)   : 200
Age Out Suppression (sec)    : 20
Age Out Dual Band (sec)      : 60
Client RSSI (dBm)            : 80
```

# show wireless client

To see the summary of the classified devices, use the **show wireless client** command.

**show wireless client device** {**cache** | **count** | **summary** } | **{steering**} [**chassis** {*chassis-number* | **active** | **standby** }]**R0**

## Syntax Description

| | |
|---|---|
| **device** | Shows classified devices. |
| **steering** | Wireless client steering information |
| **cache** | Shows the cached classified device summary. |
| **count** | Shows the wireless device count. |
| **summary** | Shows the active classified device summary. |
| *chassis-number* | Chassis number. Valid range is 1–2. |
| **active** | Active instance. |
| **standby** | Standby instance. |
| **R0** | Route-Processor slot 0. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see the 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-addressdetail** 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

## Usage Guidelines

The Client Scan Reports section in the output of the **show wireless client mac-address detail** is populated only for the following Apple devices:

- Any iPhone 7 and running iOS 11.0 or higher
- Any iPad after iPad Pro (1st gen, 12.9-inch, 2015) and running iOS 11.0 or higher

Other client devices, even if it supports 802.11k or is Wi-Fi Agile Multiband (MBO) certified, are not currently supported to populate the Client Scan Reports section.

Client ACLs shown under **show wireless client mac-address** <*mac address*> **detail** are ACLs applied on the client in Flexconnect local authentication case with MAB+Web authentication WLAN with AAA override enabled. This is applicable only for Express Wi-Fi by Facebook Policy on Controller. For more information about Facebook policy, see Express Wi-Fi by Facebook.

From Cisco IOS XE Amsterdam 17.3.1 onwards, the controller retains client session for 10 seconds. This feature is applicable for clients in the RUN state and is supported on central authentication with local and flex mode.

In idle state, 10 sec represents idle state timeout and 09 sec represent remaining time out of 10 sec. An example is given below:

```
Idle state timeout : 10 sec (Remaining time: 09 sec)
```

### Examples

The following example shows how to see detailed client information using its MAC address:

```
Device# show wireless client mac-address 98-XX-7B-XX-EF-XX detail
```

# show wireless client mac-address (Call Control)

To view call control information related to clients, use the **show wireless client mac-address** command in privileged EXEC mode.

**show wireless client mac-address** *mac-address* **call-control call-info**

## Syntax Description

| | |
|---|---|
| *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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to display call control and IP-related information about a client:

```
Device# show wireless client mac-address  30e4.db41.6157 call-control call-info
Client MAC Address        : 30E4DB416157

Call 1 Statistics

Uplink IP Address         : 209.165.200.225
Downlink IP Address       : 209.165.200.226
Uplink Port               : 29052
Downlink Port             : 27538
Call ID                   : c40acb4d-3b3b0.3d27da1e-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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to display the TCLAS and user priority-related information about a client:

```
Device# show wireless client mac-address 30e4.db41.6157 tclas
MAC Address      UP TID Mask Source IP Addr  Dest IP Addr    SrcPort DstPort Proto
----------------------------------------------------------------------------------
30e4.db41.6157    4   4   95 167838052       2164326668      5060     5060      6
30e4.db41.6157    6   1   31 0               2164326668      0        27538    17
```

# show wireless client mac-address mobility history

To see roam history of an active client in subdomain, use the **show wireless client mac-address** *mac-address* **mobility history** command.

**show wireless client mac-address** *mac-address* **mobility history**[**chassis** {*chassis-number* | **active** | **standby**} **R0**] |**events** [**chassis** {*chassis-number* | **active** | **standby**} **R0**]]

## Syntax Description

| | |
|---|---|
| *mac-address* | MAC address of the client. |
| *chassis-number* | Chassis number as either 1 or 2. |
| **active R0** | Active instance of the client in Route-processor slot 0. |
| **standby R0** | Standby instance of the client in Route-processor slot 0. |
| **events** | Shows client FSM event history. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

This example shows how to see roam history of an active client in subdomain:

```
Device# show wireless client mac-address 00:0d:ed:dd:35:80 mobility history
```

# show wireless client summary

To display a summary of active clients associated with the controller, use the **show wireless client summary** command in privileged EXEC mode.

**show wireless client summary**

### Syntax Description

This command has no arguments or keywords.

### Command Default

No default behavior or values.

### Command Modes

Privileged EXEC

### Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

### Usage Guidelines

The following is sample output from the **show wireless client summary** command:

Use the **show wireless exclusionlist** command to display clients on the exclusion list.

```
Device# show wireless client summary

Number of Clients: 1

MAC Address       AP Name                 Type ID  State  Protocol  Method  Role
-------------------------------------------------------------------------------
6c40.0899.0466    9115i-r4-sw2-te1-0-37   WLAN 7   Run    11ac      None    Local
```

# show wireless client timers

To display 802.11 system timers, use the **show wireless client timers** command in privileged EXEC mode.

**show wireless client timers**

## Syntax Description

This command has no arguments or keywords.

## Command Default

No default behavior or values.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

The following is sample output from the **show wireless client timers** command:

```
Device# show wireless client timers
 Authentication Response Timeout (seconds)      : 10
```

# show wireless country

To display the configured country and the radio types supported, use the **show wireless country** command in privileged EXEC mode.

**show wireless country** {**channels** | **configured** | **supported** [**tx-power**]}

## Syntax Description

| | |
|---|---|
| **channels** | Displays the list of possible channels for each band, and the list of channels allowed in the configured countries. |
| **configured** | Display configured countries. |
| **supported tx-power** | Displays the list of allowed Tx powers in each supported country. |

## Command Default

No default behavior or values.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

The following is sample output from the **show wireless country channels** command:

```
Device# show wireless country channels
  Configured Country.............................: US  - United States
      KEY: * = Channel is legal in this country and may be configured manually.
           A = Channel is the Auto-RF default in this country.
           . = Channel is not legal in this country.
           C = Channel has been configured for use by Auto-RF.
           x = Channel is available to be configured for use by Auto-RF.
         (-,-) = (indoor, outdoor) regulatory domain allowed by this country.
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-
    802.11bg     :
    Channels     :                   1 1 1 1 1
                 : 1 2 3 4 5 6 7 8 9 0 1 2 3 4
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 (-A   ,-AB  )  US  :  A * * * * A * * * * A . . .
 Auto-RF         : . . . . . . . . . . . . . .
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 802.11a         :                         1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
 Channels        : 3 3 3 4 4 4 4 4 5 5 6 6 0 0 0 1 1 2 2 2 3 3 4 4 5 5 6 6
                 : 4 6 8 0 2 4 6 8 2 6 0 4 0 4 8 2 6 0 4 8 2 6 0 9 3 7 1 5
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 (-A   ,-AB  )  US  :  . A . A . A . A A A A A * * * * * . . . * * * A A A A *
 Auto-RF         : . . . . . . . . . . . . . . . . . . . . . . . . . . . .
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 4.9GHz 802.11a  :
   Channels      :                   1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2
                 : 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 US (-A   ,-AB  ): * * * * * * * * * * * * * * * * * * * A * * * * * A
 Auto-RF         : . . . . . . . . . . . . . . . . . . . . . . . . . .
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

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
                 : 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  .
 (-E   ,-E   )  AL  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-A   ,-AR  )  AR  :  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  .
 (-A   ,-NA  )  AU  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
 (-E   ,-    )  BA  :  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  .
 (-E   ,-E   )  BG  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-    )  BH  :  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  .  .  .
 (-A   ,-AR  )  BR  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
 (-E   ,-    )  BY  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-A   ,-ABN )  CA  :  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  .  .  .
 (-E   ,-E   )  CH  :  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  .
 (-E   ,-E   )  CM  :  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  .
 (-A   ,-AR  )  CO  :  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  .  .  .
 (-E   ,-E   )  CY  :  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  .
 (-E   ,-E   )  DE  :  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  .
 (-A   ,-ABN )  DO  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
 (-E   ,-    )  DZ  :  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  .  .  .
 (-E   ,-E   )  EE  :  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  .
 (-E   ,-E   )  ES  :  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  .
 (-E   ,-E   )  FR  :  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  .
 (-E   ,-E   )  GI  :  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  .
 (-A   ,-NA  )  HK  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
 (-E   ,-    )  HR  :  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  .
 (-E   ,-ER  )  ID  :  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  .
 (-EI  ,-IE  )  IL  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
```

```
(-I   ,-I   )  ILO :   .  .  .  . 20 20 20 20 20 20 20 20 20  .
(-A   ,-AN  )  IN  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-E   ,-E   )  IQ  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  IS  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  IT  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-JPU ,-JPU )  J2  :  23 23 23 23 23 23 23 23 23 23 23 23 23 23
(-JPU ,-JPU )  J3  :  23 23 23 23 23 23 23 23 23 23 23 23 23 23
(-JPQU,-PQ  )  J4  :  23 23 23 23 23 23 23 23 23 23 23 23 23 23
(-E   ,-    )  JO  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-JPU ,-JPU )  JP  :  23 23 23 23 23 23 23 23 23 23 23 23 23 23
(-ACE ,-ACEK)  KE  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  KN  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-ACE ,-ACEK)  KR  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  KW  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  KZ  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  LB  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  LI  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,     )  LK  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  LT  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  LU  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  LV  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  MC  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  ME  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  MK  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,     )  MO  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  MT  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-A   ,-NA  )  MX  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-ACE ,-AEC )  MY  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  NL  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  NO  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-A   ,-NA  )  NZ  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-E   ,-E   )  OM  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-A   ,-AR  )  PA  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-A   ,-AR  )  PE  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-A   ,-ABN )  PH  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-A   ,-ABN )  PH2 :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-E   ,-E   )  PK  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  PL  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-A   ,-A   )  PR  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-E   ,-E   )  PT  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-A   ,-A   )  PY  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-E   ,-E   )  QA  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  RO  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  RS  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-AER ,-ER  )  RU  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-AE  ,-AE  )  SA  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  SE  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-SE  )  SG  :  20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-E   ,-E   )  SI  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  SK  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-ER  )  TH  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  TN  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-EI  ,-E   )  TR  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-A   ,-ANT )  TW  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-E   ,-E   )  UA  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-A   ,-AB  )  US  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-A   ,-AB  )  US2 :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-A   ,-AB  )  USL :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-A   ,-    )  USX :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-A   ,-A   )  UY  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-A   ,-AR  )  VE  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-E   ,-E   )  VN  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  ZA  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
```

# show wireless detail

To display the details of the wireless parameters configured, use the **show wireless detail** command in privileged EXEC mode.

**show wireless detail**

## Syntax Description

This command has no arguments or keywords.

## Command Default

No default behavior or values.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

The following parameters are displayed:

- The wireless user idle timeout
- The controller configured RF group name
- Fast SSID change

The following is sample output from the **show wireless detail** command:

```
Device# show wireless detail
User Timeout                  : 300
RF network                    : default
Fast SSID                     : Disabled
```

# show wireless dhcp relay statistics

To configure the wireless DHCP relay on the AP, use the **show wireless dhcp relay statistic** command.

**show wireless dhcp relay statistic**

### Syntax Description

| | |
|---|---|
| *A.B.C.D* | Indicates the target IPv4 address. |

### Command Default

None

### Command Modes

Privileged EXEC (#)

### Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 17.3.1 | This command was introduced. |

### Examples

The following example shows how to configure the wireless DHCP relay on the AP:

```
Device# show wireless dhcp relay statistics ip-address 10.1.1.1
```

# show wireless dot11h

To see 802.11h configuration details, use the **show wireless dot11h** command.

**show wireless dot11h** [ **chassis** {*chassis-number* | **active** | **standby**} **R0** ]

## Syntax Description

| | |
|---|---|
| *chassis-number* | Chassis number. Valid range is 1–2. |
| **active** | Active instance. |
| **standby** | Standby instance. |
| **R0** | Route-Processor slot 0. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see the 802.11h configuration details:

```
Device# show wireless dot11h
```

# show wireless dtls connections

To display the Datagram Transport Layer Security (DTLS) server status, use the **show wireless dtls connections** command in privileged EXEC mode.

**show wireless dtls connections**

## Syntax Description

This command has no arguments or keywords.

## Command Default

No default behavior or values.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

The following is sample output from the **show wireless dtls connections** command:

```
Device# show wireless dtls connections
 AP Name          Local Port   Peer IP    Peer Port  Ciphersuite
----------------------------------------------------------------------
  AP-2       Capwap_Ctrl   10.0.0.16     52346      TLS_RSA_WITH_AES_128_CBC_SHA
  AP-3       Capwap_Ctrl   10.0.0.17     52347      TLS_RSA_WITH_AES_128_CBC_SHA
```

# show wireless exclusionlist

To see the wireless exclusion list, use the **show wireless exclusionlist** command.

**show wireless exclusionlist** [**client mac-address** *client-mac-addr* **detail** ] [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

## Syntax Description

| | |
|---|---|
| *client-mac-addr* | Client MAC address. |
| *chassis-number* | Enter the chassis number as either 1 or 2. |
| **active R0** | Active instance of the configuration in Route-processor slot 0. |
| **standby R0** | Standby instance of the configuration in Route-processor slot 0. |

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see the wireless exclusion list:

```
Device# show wireless exclusionlist

Excluded Clients

MAC Address       Description          Exclusion Reason              Time Remaining
-----------------------------------------------------------------------------------------
10da.4320.cce9                         Client Policy  failure         59
```

# show wireless fabric summary

To view the fabric status, use the **show wireless fabric summary** command.

**show wireless fabric summary**

### Syntax Description

This command has no arguments.

### Command Default

None

### Command Modes

Global configuration

### Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |
| Cisco IOS XE 17.14.1 | The output of the command was modified to include IPv6 address. |

This example shows how to view fabric status:

```
Device# show wireless fabric summary
Fabric Status      : Enabled


Control-plane:
Name                             IP-address        Key                              Status
------------------------------------------------------------------------------------------
test-map                         10.12.13.14       test1                            Down


Fabric VNID Mapping:
  Name               L2-VNID        L3-VNID        IP Address             Subnet
Control plane name
------------------------------------------------------------------------------------------

  test1               12             10             10.6.8.9            255.255.255.236
 test2
```

This example shows how to view fabric status for IPv6:

```
Device# show wireless fabric summary
Fabric Status      : Enabled


Control-plane:
Name                                IP-address                                Key
                         Status
------------------------------------------------------------------------------------------
default-control-plane               2001:192:168:1::3                         cisco123
                         Up


Fabric VNID Mapping:
  Name               L2-VNID       L3-VNID       IP Address
  Subnet                                     Control plane name
------------------------------------------------------------------------------------------
```

```
130_120_0_INFRA    8188          4097          2003:2000:130:120::1
ffff:ffff:ffff:ffff::                      default-control-plane
```

# show wireless fabric client summary

To see the summary of a fabric enabled wireless client, use the **show wireless fabric client summary** command.

**show wirelessv fabric client summary**

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |
| Cisco IOS XE 17.14.1 | The output of the command was modified to include IPv6 address. |

### Examples

The following example shows how to see the fabric enabled wireless client summary:

```
Device# show wireless fabric client summary
```

The following example shows how to see the fabric enabled wireless client summary for IPv6:

```
Device# show wireless fabric client summary
Number of Fabric Clients : 2
MAC Address          AP Name                Type       ID      State      Protocol     Method
  L2 VNID      RLOC IP

2c33.7a5b.8fc5     APC4F7.D54D.0B94       WLAN       22       Run        11n(2.4)      None
    8190    1100:10:10:10:1:1:1:6
40ec.995a.434e    APC4F7.D54D.0B94        WLAN       20       Run        11ac          None
    8190    1100:10:10:10:1:1:1:6
```

# show wireless fabric vnid mapping

To view all the VNID mapping details, use the **show wireless fabric vnid mapping** command.

**show wireless fabric vnid mapping**

## Syntax Description

This command has no arguments.

## Command Default

None

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view all the VNID mapping details:

```
Device# show wireless fabric vnid mapping
Fabric VNID Mapping:
  Name               L2-VNID        L3-VNID        IP Address              Subnet
Control plane name
------------------------------------------------------------------------------------------


  test1               12             10             10.6.8.9             255.255.255.236
 test2
```

# show wireless flow-control

To display the information about flow control on a particular channel, use the **show wireless flow-control** command in privileged EXEC mode.

**show wireless flow-control** *channel-id*

## Syntax Description

| | |
|---|---|
| *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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

The following is sample output from the **show wireless flow-control** *channel-id* command:

```
Device# show wireless flow-control 3
Channel Name                           : CAPWAP
FC State                               : Disabled
Remote Server State                    : Enabled
Pass-thru Mode                         : Disabled
EnQ Disabled                           : Disabled
Queue Depth                            : 2048
Max Retries                            : 5
Min Retry Gap (mSec)                   : 3
```

# show wireless flow-control statistics

To display the complete information about flow control on a particular channel, use the **show wireless flow-control statistics** command in privileged EXEC mode.

**show wireless flow-control** *channel-id* **statistics**

## Syntax Description

| | |
|---|---|
| *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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

The following is sample output from the **show wireless flow-control** *channel-id* **statistics** command:

```
Device# show wireless flow-control 3 statistics
 Channel Name                                 : CAPWAP
# of times channel went into FC               : 0
# of times channel came out of FC             : 0
Total msg count received by the FC Infra      : 1
Pass-thru msgs send count                     : 0
Pass-thru msgs fail count                     : 0
# of msgs successfully queued                 : 0
# of msgs for which queuing failed            : 0
# of msgs sent thru after queuing             : 0
# of msgs sent w/o queuing                    : 1
# of msgs for which send failed               : 0
# of invalid EAGAINS received                 : 0
Highest watermark reached                     : 0
# of times Q hit max capacity                 : 0
Avg time channel stays in FC (mSec)           : 0
```

# show wireless load-balancing

To display the status of the load-balancing feature, use the **show wireless load-balancing** command in privileged EXEC mode.

**show wireless load-balancing**

## Syntax Description

This command has no arguments or keywords.

## Command Default

No default behavior or values.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

The following is sample output from the **show wireless load-balancing** command:

```
 > show wireless load-balancing
Aggressive Load Balancing............................: per WLAN enabling
Aggressive Load Balancing Window (clients).................:: 5
Aggressive Load Balancing Denial Count.....................:: 3

Statistics
Total Denied Count (clients)................................:: 0
Total Denial Sent (messages)................................:: 0
Exceeded Denial Max Limit Count (times).....................:: 0
None 5G Candidate Count (times).............................:: 0
None 2.4G Candidate Count (times)...........................:: 0
```

# show wireless media-stream client detail

To see the media stream clients information by stream name, use the **show wireless media-stream client detail** command.

**show wireless media-stream client detail**

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see media stream clients information by stream name:

```
Device# show wireless media-stream client detail
```

# show wireless media-stream group

To display the wireless media-stream group information, use the **show wireless media-stream group** command.

**show wireless media-stream group** {**detail** *groupName* | **summary**}

### Syntax Description

| | |
|---|---|
| **detail** *groupName* | Display media-stream group configuration details of the group mentioned in the command. |
| **summary** | Display media-stream group configuration summary |

### Command Default

None

### Command Modes

User EXEC mode or Privileged EXEC mode

### Usage Guidelines

None.

The following is a sample output of the **show wireless media-stream group detail GRP1** command.

```
Device#show wireless media-stream group detail GRP1
```

```
Device#show wireless media-stream group detail GRP1
Media Stream Name : GRP1
Start IP Address : 234.1.1.1
End IP Address : 234.1.1.5
RRC Parameters:
Avg Packet Size(Bytes) : 1200
Expected Bandwidth(Kbps) : 1000
Policy : Admitted
RRC re-evaluation : Initial
QoS : video
Status : Multicast-direct
```

The following is a sample output of the **show wireless media-stream group summary** command.

```
Device#show wireless media-stream group summary
Number of Groups:: 1
Stream Name          Start IP                                 End IP
Status
-----------------------------------------------------------------------------------------
GRP1                 234.1.1.1                                234.1.1.5
Enabled
```

# show wireless media-stream message details

To see the wireless multicast-direct session announcement message details, use the **show wireless media-stream message details** command.

**show wireless media-stream message details**

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see the wireless multicast-direct session announcement message details:

```
Device# show wireless media-stream message details
```

# show wireless mobility controller ap

To display the list of access points which have joined the sub-domain, use the **wireless mobility controller ap** command.

**show wireless mobility controller ap**

## Syntax Description

| | |
|---|---|
| **ap** | Show joined Access Point in sub-domain. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Denali 16.3.1 | This command was introduced. |

## Usage Guidelines

None

This example shows how to list the access points which have joined the sub-domain.

```
Device#show wireless mobility controller ap
Number of AP entries in the sub-domain     : 2

AP name                           AP radio MAC      Controller IP     Location
-------------------------------------------------------------------------------------------
bos2kk                            00f2.8c42.f520    default-group     default-group
IosAP1                            34ed.522f.7e60    default-group     default-group
```

# show wireless media-stream multicast-direct state

To see the state of the wireless multicast-direct configuration, use the **show wireless media-stream multicast-direct state** command.

**show wireless media-stream multicast-direct state**

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see the state of the wireless multicast-direct configuration:

```
Device# show wireless media-stream multicast-direct state
```

# show wireless mesh ap

To see the mesh AP related information, use the **show wireless mesh ap** command.

**show wireless mesh ap** { **summary** | **tree** | **backhaul** } [ **chassis** { *chassis-number* | **active** | **standby** } **R0** ]

## Syntax Description

| | |
|---|---|
| **summary** | Shows the summary of all connected mesh APs. |
| **tree** | Shows the Mesh AP tree. |
| **backhaul** | Shows the mesh APs backhaul info. |
| *chassis-number* | Enter the chassis number as either 1 or 2. |
| **active R0** | Active instance of the configuration in Route-processor slot 0. |
| **standby R0** | Standby instance of the configuration in Route-processor slot 0. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see the summary of all connected mesh APs:

```
Device# wireless mesh ap summary
```

# show wireless mesh ap tree

To see the mesh AP tree, use the **show wireless mesh ap tree** command.

**show wireless mesh ap tree**

### Syntax Description

This command has no keywords or arguments.

### Command Default

None

### Command Modes

Privileged EXEC

### Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

### Example

The following example shows how to view the wireless mesh AP tree:

```
Device # show wireless mesh ap tree
```

# show wireless mesh ap tree

To see the mesh AP tree, use the **show wireless mesh ap tree** command.

**show wireless mesh ap tree**

## Syntax Description

This command has no keywords or arguments.

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

### Example

The following example shows how to view the wireless mesh AP tree:

```
Device # show wireless mesh ap tree
```

# show wireless mesh config

To see the mesh configurations, use the **show wireless mesh config** command.

**show wireless mesh config** [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

## Syntax Description

| | |
|---|---|
| **config** | Shows the mesh configurations. |
| *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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see the mesh configurations:

```
Device# wireless mesh config
```

# show wireless mesh neighbor

To see the neighbors of all connected mesh APs, use the **show wireless mesh neighbor** command.

**show wireless mesh neighbor** [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

## Syntax Description

| | |
|---|---|
| **neighbor** | Shows the neighbors of all connected mesh APs. |
| *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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

## Usage Guidelines

Definition of the field State is as follows:

- **UPDATED**: Adjacency is reachable: communication is symmetric, we can exchange frames with that AP.
- **NEIGH**: Adjacency is parent capable. Local criterion: reachability, strict BGN config, valid cost, potential loops, and so on.
- **CHILD**: Adjacency is actually a child mesh AP (associated to the considered AP).
- **PARENT**: Adjacency is actually the parent mesh AP.
- **DEFAULT**: Adjacency BGN is different than our backhaul configured one.
- **BLOCK**: Adjacency is currently blocklisted due to: auth failures, capwap teardown, and so on.

### Examples

The following example shows how to see the neighbors of all connected mesh APs:

```
Device# show wireless mesh neighbor

AP Name/Radio             Channel   Rate      Link-snr   Flags   State
------------------------------------------------------------------------------------------


AP Name : Mesh-AP01

54:9f:c6:fa:5c:71         149       auto      0          40
```

```
b0:c5:3c:e5:d9:71          149       auto      22          49      UPDATED NEIGH
e8:eb:34:d5:88:d1          149       auto      0           40
e8:eb:34:d5:8d:d1          149       auto      18          49      UPDATED CHILD
e8:eb:34:d5:94:d1          149       auto      37          4b      UPDATED NEIGH PARENT
e8:eb:34:d5:d3:11          149       auto      31          49      UPDATED NEIGH
e8:eb:34:d5:d8:91          149       auto      0           41      UPDATED
e8:eb:34:d5:da:31          149       auto      18          49      UPDATED NEIGH
e8:eb:34:d5:da:51          149       auto      0           1040    DEFAULT
e8:eb:34:d5:dc:d1          149       auto      9           49      UPDATED NEIGH
e8:eb:34:d5:ef:51          149       auto      0           40
e8:eb:34:d5:f6:51          149       auto      9           49      UPDATED NEIGH
e8:eb:34:d5:fd:51          149       auto      21          49      UPDATED NEIGH
ec:ce:13:9a:89:91          149       auto      19          49      UPDATED NEIGH
ec:ce:13:d7:6f:91          149       auto      18          49      UPDATED NEIGH
ec:ce:13:d7:75:71          149       auto      19          49      UPDATED NEIGH
ec:ce:13:d7:87:91          149       auto      0           41      UPDATED
ec:ce:13:d7:8e:51          149       auto      6           49      UPDATED NEIGH
```

# show wireless 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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to display a summary of the mobility manager:

```
Device (config)# show wireless mobility ap-list

AP name                           AP radio MAC      Controller IP     Learnt from
----------------------------------------------------------------------------------------
TSIM_AP-101                       0000.2000.6600    9.9.9.2           Self
TSIM_AP-102                       0000.2000.6700    9.9.9.2           Self
TSIM_AP-103                       0000.2000.6800    9.9.9.2           Self
TSIM_AP-400                       0000.2001.9100    9.9.9.2           Self
TSIM_AP-402                       0000.2001.9300    9.9.9.2           Self
TSIM_AP-403                       0000.2001.9400    9.9.9.2           Self
TSIM_AP-406                       0000.2001.9700    9.9.9.2           Self
TSIM_AP-407                       0000.2001.9800    9.9.9.2           Self
TSIM_AP-409                       0000.2001.9a00    9.9.9.2           Self
```

# show wireless mobility peer ip

To see the details of the mobility peer using its IP address, use the **show wireless mobility peer ip** command.

**show wireless mobility peer ip** *ip-address*

## Syntax Description

| | |
|---|---|
| *ip-address* | Mobility peer IPv4 IP address. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see the details of the wireless mobility peer using its IP address:

```
Device# show wireless mobility peer ip 209.165.200.224
```

# show wireless multicast group summary

To see the wireless multicast group summary, use the **show wireless multicast group summary** command.

**show wireless multicast group summary**

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see the summary of the wireless multicast group:

```
Device# show wireless multicast group summary
```

# show wireless mobility summary

To see the wireless mobility manager summary, use the **show wireless mobility summary** command.

**show wireless mobility summary**

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see the wireless mobility manager's summary:

```
Device# show wireless mobility summary
```

# show wireless multicast

To display wireless multicast information, use the **show wireless multicast** command in privileged EXEC mode.

**show wireless multicast** [**source** *source-ip* **group** *group-ip* **vlan** *vlan-id* | **group** *group-ip* **vlan** *vlan-id*]

### Syntax Description

| | |
|---|---|
| **source** *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 mutlicast traffic. |
| **vlan** *vlan-id* | Displays the client information on VLAN with the specific VLAN ID. |

### Command Default

None

### Command Modes

Privileged EXEC

### Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

### Usage Guidelines

None

This example shows how to display the 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 | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

None.

### Examples

This example shows how to display the wireless-multicast non-ip group summary.

```
Device# show wireless multicast group summary
```

# show wireless performance

To display aggressive load balancing configuration, use the **show wireless performance** command in privileged EXEC mode.

**show wireless performance** {**ap** | **client**} **summary**

## Syntax Description

| | |
|---|---|
| **ap summary** | Displays aggressive load balancing configuration of access points configured to the controller. |
| **client summary** | Displays aggressive load balancing configuration details of the clients. |

## Command Default

No default behavior or values.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

The following is sample output from the **show wireless performance ap summary** command.

```
Device# show wireless performance ap summary
Number of APs:
```

The following is sample output from the **show wireless performance client summary** command.

```
Device# show wireless performance client summary
Number of Clients:

MAC Address        AP Name           Status        WLAN/Guest-Lan Auth Protocol Port Wired
------------------------------------------------------------------------------------------
```

# show wireless pmk-cache

To display information about the pairwise master key (PMK) cache, use the **show wireless pmk-cache** command in privileged EXEC mode.

**show wireless pmk-cache**[**mac-address** *mac-addr*]

## Syntax Description

| | |
|---|---|
| **mac-address** *mac-addr* | (Optional) Information about a single entry in the PMK cache. |

## Command Default

No default behavior or values.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

The following is sample output from the **show wireless pmk-cache mac-address** command:

```
Device# show wireless pmk-cache mac-address H.H.H
Number of PMK caches in total : 0
```

# show wireless probe

To display the advanced probe request filtering configuration and the number of probes sent to the WLAN controller per access point per client and the probe interval in milliseconds, use the **show wireless probe** command in privileged EXEC mode.

**show wireless probe**

## Syntax Description

This command has no arguments or keywords.

## Command Default

No default behavior or values.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

The following is sample output from the **show wireless probe** command:

```
Device# show wireless probe
Probe request filtering                          : Enabled
Number of probes per client per radio fwd from AP: 2
Probe request rate-limiting interval             : 500 msec
Aggregate probe request interval                 : 500 msec
```

# show wireless profile airtime-fairness mapping

To view the ATF policy mapping with the wireless profiles, use the **show wireless profile airtime-fairness mapping** command.

**show wireless profile airtime-fairness mapping**

### Syntax Description

This command has no arguments.

### Command Default

None

### Command Modes

Global configuration

### Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the ATF policy mapping with the wireless profiles:

```
Device# show wireless profile airtime-fairness mapping
Policy Profile                    Band      ATF Policy                       Weight
Client Sharing    Availability
------------------------------------------------------------------------------------------
WGB                               2.4GHz                                      -         -
                No
WGB                               5GHz                                        -         -
                No
Policy1                           2.4GHz                                      -         -
                No
Policy1                           5GHz                                        -         -
                No
Test WBG                          2.4GHz                                      -         -
                No
Test WBG                          5GHz                                        -         -
                No
profile-name                      2.4GHz    atf-policy-name                   5
Enabled           Yes
```

# show wireless profile airtime-fairness summary

To view the summary of air time fairness profiles, use the **show wireless profile airtime-fairness summary** command.

**show wireless profile airtime-fairness summary**

## Syntax Description

This command has no arguments.

## Command Default

None

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the summary of air time fairness profiles:

```
Device# show wireless profile airtime-fairness summary
Policy Id      Policy Name                          Weight      Client Sharing
--------------------------------------------------------------------------
1              atf-policy-name                       5           Enabled
```

# show wireless profile ap packet-capture

To view the AP packet capture information, use the **show wireless profile ap packet-capture** command.

**show wireless profile ap packet-capture** {**detailed** *profile-name* | **summary**}

## Syntax Description

| | |
|---|---|
| *profile-name* | AP packet capture profile. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

### Example

The following example shows how to view the AP packet capture information:

```
Device# show wireless profile ap packet-capture summary
Number of AP packet capture profiles: 3

Profile Name               Buffer   Duration(M Packet Len FTP IP
----------------------------------------------------------------------
test                        1200        20         0      9.1.0.101
test1                       2048        10         0      0.0.0.0
tets1                       1024        10         0      0.0.0.0
```

### Example

The following example shows how to view the detailed AP packet capture information of an AP profile:

```
Device# show wireless profile ap packet-capture detailed test1

Profile Name : test1
Description  :
---------------------------------------------------
Buffer Size       : 2048 KB
Capture Duration  : 10 Minutes
Truncate Length   : packet length
FTP Server IP     : 0.0.0.0
FTP path          :
FTP Username      :

Packet Classifiers
  802.11 Control  : Enabled
  802.11 Mgmt     : Enabled
  802.11 Data     : Disabled
  Dot1x           : Disabled
```

```
ARP             : Disabled
IAPP            : Disabled
IP              : Disabled
TCP             : Disabled
TCP port        : all
UDP             : Disabled
UDP port        : all
Broadcast       : Disabled
Multicast       : Disabled
```

# show wireless profile fabric detailed

To view the details of a given fabric profile name, use the **show wireless profile fabric detailed** command.

**show wireless profile fabric detailed** *fabric_profile_name*

## Syntax Description

This command has no arguments.

## Command Default

None

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the details of a given fabric profile name:

```
Device# show wireless profile fabric detailed test1
Profile-name      : test-fabric
VNID              : 12
SGT               : 5
```

# show wireless profile flex

To see the flex parameters of an wireless profile, use the **show wireless profile flex** command.

**show wireless profile flex** { **detailed** *flex-profile-name* **chassis** {*chassis-number* | **active** | **standby** }**R0** } | **summary chassis** {*chassis-number* | **active** | **standby**}**R0**}

## Syntax Description

| | |
|---|---|
| **detailed** | Shows the flex-profile detailed parameters |
| **summary** | Show the flex-profile summary. |
| *chassis-number* | Chassis number. Valid range is 1–2. |
| **active** | Active instance. |
| **standby** | Standby instance. |
| **R0** | Route-Processor slot 0. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see the flex parameter's summary of the wireless profile:

```
Device# show wireless profile flex summary
```

# show wireless profile policy detailed

To display the wireless policy profile details, use the **show wireless profile policy detailed** command.

**show wireless profile policy detailed** *policy-profile-name*

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

None

**Command Modes**

Privilege EXEC (#)

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS XE Amsterdam 17.2.1 | This command was introduced. |

### Example

This example displays the wireless policy profile details:

```
Device#show wireless profile policy detailed policy-profile-name
```

# show wireless redundancy statistics

To see the high availability statistics, use the **show wireless redundancy statistics** command.

**show wireless redundancy statistics** {**ap-group** | **wncdallchassis** {*chassis-num* | **active** | **standby**}**R0**}
{**ap-recovery** | {*instance-id* | **all** | **chassis** {*chassis-num* | **active** | **standby**}**R0**}}
{**client-group** | **wncdallchassis** {*chassis-num* | **active** | **standby**}**R0**}
{**client-recovery** | {**mobilityd** | **sisf**}**chassis** {*chassis-num* | **active** | **standby**}**R0**}
{**wncd** | {*instance-id* | **all** | **chassis** {*chassis-num* | **active** | **standby**}**R0**}}

## Syntax Description

| | |
|---|---|
| *chassis-number* | Enter the chassis number as either 1 or 2. |
| **active R0** | Active instance of the configuration in Route-processor slot 0. |
| **standby R0** | Standby instance of the configuration in Route-processor slot 0. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see all the statistics for WNCD :

# show wireless rfid

To display RFID tag information, use the **show wireless rfid** command in privileged EXEC mode.

**show wireless rfid** {**client** | **detail** *rfid-mac-address* | **stats** | **summary**}

## Syntax Description

| | |
|---|---|
| **client** | Displays the summary of RFID tags that are clients. |
| **detail** | Displays information about a particular RFID tag. |
| **stats** | Displays RFID statistics. |
| **summary** | Displays summary information for all known RFID tags. |
| *rfid-mac-address* | RFID MAC address. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

### Example

This example shows how to view RFID information:

```
Device# show wireless rfid summary

Total RFID entries: : 16
Total Unique RFID entries : 16
RFID ID VENDOR Closet AP RSSI Time Since Last Heard
0012.b80a.c791 Cisco 7069.5a63.0520 -31 1 minute 40 seconds ago
0012.b80a.c953 Cisco 7069.5a63.0460 -33 2 minutes 15 seconds ago
0012.b80b.806c Cisco 7069.5a63.0260 -45 22 seconds ago
0012.b80d.e9f9 Cisco 7069.5a63.0460 -38 2 minutes 37 seconds ago
0012.b80d.ea03 Cisco 7069.5a63.0520 -43 2 minutes 38 seconds ago
0012.b80d.ea6b Cisco 7069.5a63.0460 -39 2 minutes 35 seconds ago
0012.b80d.ebe8 Cisco 7069.5a63.0520 -43 1 minute 31 seconds ago
0012.b80d.ebeb Cisco 7069.5a63.0520 -43 2 minutes 37 seconds ago
0012.b80d.ec48 Cisco 7069.5a63.0460 -42 2 minutes 16 seconds ago
0012.b80d.ec55 Cisco 7069.5a63.0520 -41 1 second ago
```

# show wireless stats client delete reasons

To verify total client delete reasons, use the **show wireless stats client delete reasons** command.

**show wireless stats client delete reasons**

## Syntax Description

This command has no keywords or arguments.

## Command Default

None

## Command Modes

Privileged EXEC(#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Amsterdam 17.1.1 | This command was introduced. |

This example shows how to verify the total client delete reasons:

```
Device# show wireless stats client delete reasons

Total client delete reasons
---------------------------
Controller deletes
---------------------------
---------------------------
No Operation                                                    : 0
Unknown                                                         : 0
Session Manager                                                 : 0
Connection timeout                                              : 0
Datapath plumb                                                  : 0
WPA key exchange timeout                                        : 0
802.11w MAX SA queries reached                                  : 0
Client deleted during HA recovery                               : 0
Inter instance roam failure                                     : 0
Inter instance roam success                                     : 0
Inter controller roam success                                   : 0
Due to mobility failure                                         : 0
NAS error                                                       : 0
Policy Manager internal error                                   : 0
80211v smart roam failed                                        : 0
DOT11v association failed                                       : 0
DOT11r pre-authentication failure                               : 0
SAE authentication failure                                      : 0
DOT11 failure                                                   : 0
DOT11 SAE invalid message                                       : 0
DOT11 denied data rates                                         : 0
802.11v Client RSSI lower than the association RSSI threshold   : 0
invalid QoS parameter                                           : 0
DOT11 IE validation failed                                      : 0
DOT11 group cipher in IE validation failed                      : 0
DOT11 invalid pairwise cipher                                   : 0
DOT11 invalid AKM                                               : 0
DOT11 unsupported RSN version                                   : 0
DOT11 invalid RSNIE capabilities                                : 0
DOT11 received invalid PMKID in the received RSN IE             : 0
```

```
DOT11 received invalid PMK length                               : 0
DOT11 invalid MDIE                                              : 0
DOT11 invalid FT IE                                             : 0
DOT11 AID allocation conflicts                                  : 0
AVC client re-anchored at the foreign controller                : 0
Client EAP ID timeout                                           : 0
Client DOT1x timeout                                            : 0
Malformed EAP key frame                                         : 0
EAP key install bit is not expected                             : 0
EAP key error bit is not expected                               : 0
EAP key ACK bit is not expected                                 : 0
Invalid key type                                                : 0
EAP key secure bit is not expected                              : 0
key description version mismatch                                : 0
wrong replay counter                                            : 0
EAP key MIC bit expected                                        : 0
MIC validation failed                                           : 0
MAC theft                                                       : 0
IP theft                                                        : 0
Policy bind failure                                             : 0
Web authentication failure                                      : 0
802.1X authentication credential failure                        : 0
802.1X authentication timeout                                   : 0
802.11 authentication failure                                   : 0
802.11 association failure                                      : 0
Manually excluded                                               : 0
DB error                                                        : 0
Anchor creation failure                                         : 0
Anchor invalid Mobility BSSID                                   : 0
Anchor no memory                                                : 0
Call admission controller at anchor node                        : 0
Supplicant restart                                              : 0
Port admin disabled                                             : 0
Reauthentication failure                                        : 0
Client connection lost                                          : 0
Error while PTK computation                                     : 0
MAC and IP theft                                                : 0
QoS policy failure                                              : 0
QoS policy send to AP failure                                   : 0
QoS policy bind on AP failure                                   : 0
QoS policy unbind on AP failure                                 : 0
Static IP anchor discovery failure                              : 0
VLAN failure                                                    : 0
ACL failure                                                     : 0
Redirect ACL failure                                            : 0
Accounting failure                                              : 0
Security group tag failure                                      : 0
FQDN filter definition does not exist                           : 0
Wrong filter type, expected postauth FQDN filter                : 0
Wrong filter type, expected preauth FQDN filter                 : 0
Invalid group id for FQDN filter valid range  1..16             : 0
Policy parameter mismatch                                       : 0
Reauth failure                                                  : 0
Wrong PSK                                                       : 0
Policy failure                                                  : 0
AAA server unavailable                                          : 0
AAA server not ready                                            : 0
No dot1x method configuration                                   : 0
Association connection timeout                                  : 0
MAC-AUTH connection timeout                                     : 0
L2-AUTH connection timeout                                      : 0
L3-AUTH connection timeout                                      : 0
Mobility connection timeout                                     : 0
static IP connection timeout                                    : 0
```

```
SM session creation timeout                                     : 0
IP-LEARN connection timeout                                     : 0
NACK IFID exists                                                : 0
Guest-LAN invalid MBSSID                                        : 0
Guest-LAN no memory                                             : 0
Guest-LAN ceate request failed                                  : 0
EoGRE Reset                                                     : 0
EoGRE Generic Join Failure                                      : 0
EoGRE HA-Reconciliation                                         : 0
Wired idle timeout                                              : 0
IP Update timeout                                               : 0
SAE Commit received in Associated State                         : 0
NACK IFID mismatch                                              : 0
EoGRE Invalid VLAN                                              : 0
EoGRE Empty Domain                                              : 0
EoGRE Invalid Domain                                            : 0
EoGRE Domain Shut                                               : 0
EoGRE Invalid Gateway                                           : 0
EoGRE All Gateways down                                         : 0
EoGRE Flex - no active gateway                                  : 0
EoGRE Rule Matching error                                       : 0
EoGRE AAA Override error                                        : 0
EoGRE client onboarding error                                   : 0
EoGRE Mobility Handoff error                                    : 0
L3 VLAN Override connection timeout                             : 0
Delete received from AP                                         : 0
QoS failure                                                     : 0
WPA group key update timeout                                    : 0
DOT11 unsupported client capabilities                           : 0
DOT11 association denied unspecified                            : 0
DOT11 AP have insufficient bandwidth                            : 0
DOT11 invalid QoS parameter                                     : 0
Client not allowed by assisted roaming                          : 0
Wired client deleted due to WGB delete                          : 0
Client Abort                                                    : 0
Mobility peer delete                                            : 0
No IP                                                           : 0
BSSID down                                                      : 0
DOT11 QoS policy                                                : 0
Roam across policy profile deny                                 : 0
4WAY handshake failure - M1 issue                               : 0
4WAY handshake failure - M3 issue                               : 0
Exclusion policy template fail                                  : 0
DOT11 Cipher Suite Rejected                                     : 0
WLAN-ID mismatch in access accept failures                      : 0
EasyPSK AAA unknown error                                       : 0
EasyPSK unspecified error                                       : 0
EasyPSK PSK mismatch error                                      : 0
EasyPSK radius busy error                                       : 0
EasyPSK limit reached error                                     : 0
EasyPSK bad 802.1X frame error                                  : 0
EasyPSK missing parameter error                                 : 0
Supplicant name failure                                         : 0
User name failure                                               : 0
Service set ID failure                                          : 0
Anchor VLAN ID failure                                          : 0
PSK failure                                                     : 0
PSK mode failure                                                : 0
Interim interval failure                                        : 0
Link-local bridging VLAN failure                                : 0
Link-local bridging VLAN failure                                : 0
Maximum client limit reached on AP                              : 0
Maximum client limit reached on AP per wlan                     : 0
Maximum client limit reached on AP radio per wlan               : 0
Maximum client limit reached on AP radio                        : 0
L3 Access Roam across policy profile deny                       : 0
L3 Access Inter controller roam deny                            : 0
----------------------------
Informational Delete Reason
-----------------------------
Mobility WLAN down                                              : 0
AP upgrade                                                      : 0
L3 authentication failure                                       : 0
AP down/disjoin                                                 : 0
MAC authentication failure                                      : 0
Due to SSID change                                              : 0
Due to VLAN change                                              : 0
Admin deauthentication                                          : 0
Session timeout                                                 : 0
Idle timeout                                                    : 0
Supplicant request                                              : 0
Mobility tunnel down                                            : 0
DOT11v timer timeout                                            : 0
DOT11 max STA                                                   : 0
IAPP disassociation for wired client                            : 0
Wired WGB change                                                : 0
Wired VLAN change                                               : 0
WGB Wired client joins as a direct wireless client              : 0
Incorrect credentials                                           : 0
Wired client cleanup due to WGB roaming                         : 0
Radio Down                                                      : 0
Mobility failure on fast roam                                   : 0
Due to IP Zone change                                           : 0
Access denied due to Locally Administered MAC Address           : 0
-----------------------------
-----------------------------
Client initiate delete
-----------------------------
Deauthentication or disassociation request                      : 0
Client DHCP                                                     : 0
Client EAP timeout                                              : 0
Client 8021x failure                                            : 0
Client device idle                                              : 0
Client captive portal security failure                          : 0
Client decryption failure                                       : 0
Client interface disabled                                       : 0
Client user triggered disassociation                            : 0
Client miscellaneous reason                                     : 0
Unknown                                                         : 0
Client peer triggered                                           : 0
Client beacon loss                                              : 0
STA triggered PMK timeout                                  : 0
Excess ARP activity                                        : 0
Excess NDP activity                                        : 0
Unspecified QOS failure                                        : 0
Dpath encode failed                                            : 0
VRF-VLAN mismatch failures                                    : 0
-----------------------------
AP Deletes
-----------------------------
When client is sending disassociation                      : 0
Idle timeout                                               : 0
Client ACL mismatch                                        : 0
AP authentication stop                                     : 0
Association expired at AP                                  : 0
4-way handshake failed                                     : 0
DHCP timeout                                               : 0
Reassociation timeout                                      : 0
```

```
SA query timeout                                            : 0
Intra AP roam                                               : 0
Channel switch at AP                                        : 0
Bad AID                                                     : 0
AP requests for client deletion                             : 0
Interface reset                                             : 0
All on slot                                                 : 0
Link to client has changed and uplink can be reaper         : 0
Slot disable                                                : 0
MIC failure                                                 : 0
VLAN delete                                                 : 0
Channel change                                              : 0
Stop reassociation                                          : 0
Packet maximum retry                                        : 0
Transmission deauthentication                               : 0
Sensor station timeout                                      : 0
Age timeout                                                 : 0
Transmission threshold fail                                 : 0
Uplink receive timeout                                      : 0
Sensor scan next radio                                      : 0
Sensor scan other BSSID                                     : 0
Authentication timeout and web-auth timeout                 : 0
Sending deauthentication packet to client                   : 0
AP IP learn timeout                                         : 0
Flex group change                                           : 0
EAPOL log off                                               : 0
EAP request timeout                                         : 0
4way handshake failure                                      : 0
MIC validation                                              : 0
Wrong replay counter                                        : 0
AP tunnel down                                              : 0
Inter roam                                                  : 0
Unknown client                                              : 0
Reauthentication timeout                                    : 0
Continuous idle timeout                                     : 0
RLDP cleanup                                                : 0
Intra-switch roam                                           : 0
PEM cleanup                                                 : 0
RLAN Central switch                                         : 0
RLAN data path add failure                                  : 0
RLAN Delete                                                 : 0
RLAN Inactive timeout                                       : 0
RLAN MAB failure                                            : 0
CLSM No memory counter                                      : 0
CLSM BSSID mismatch                                         : 0
CLSM No ACL found                                           : 0
CLSM no parent WGB found                                    : 0
CLSM Key plumb faiure                                       : 0
CLSM Mesh key plumb failure                                 : 0
CLSM data path add fail                                     : 0
CLSM Authentication response reject                         : 0
CLSM Authentication response send failure                   : 0
CLSM Association response send failure                      : 0
CLSM association response failure with status               : 0
CLSM Webauth timer expired                                  : 0
CLSM Dot1x timer expired                                    : 0
CLSM deauthentication and disassociation send failure       : 0
Driver event Class3 received                                : 0
Driver event PsPoll when not authenticated                  : 0
Driver event ioctl error                                    : 0
Flex FT failure                                             : 0
CLSM driver add failure                                     : 0
Driver client not found                                     : 0
Driver management packet allocation failure                 : 0
Driver invalid cipher                                      : 0
Driver invalid association identifier                      : 0
Driver invalid key                                         : 0
Driver firmware set key failure                            : 0
Driver found invalid HT VHT rates                          : 0
Driver found invalid legacy rates                          : 0
Driver found no overlapping legacy rates                   : 0
Driver found maximum VHT streams                           : 0
Driver found association identifer in use                  : 0
Driver found too many association requests                 : 0
Driver found cipher attach failure                         : 0
Driver found algorithm mismatch                            : 0
Driver found invalid key length                            : 0
Driver found invalid key index                             : 0
Driver rejected association due to authentication failure  : 0
Driver found client addition to internal records failure   : 0
Driver found client association entry failure              : 0
Driver found client additions to firmware failure          : 0
Driver related internal failure                            : 0
AP limiting maximum client per AP                          : 0
AP limiting maximum client per AP radio per wlan           : 0
AP limiting maximum client per AP radio                    : 0
-------------------
PC Analytics stats:
----------------------------------------
Report Type            Processed Reports
----------------------------------------
 PC_STA_INFO          : 0
 PC_NEIGH_INFO        : 0
 PC_LOW_RSSI          : 0
 PC_TEMP_DISCONN      : 0
 PC_AP_FAILURE        : 0
 PC_UNKNOWN_AP        : 0
--------------------------------------
Report Type            Dropped Reports
--------------------------------------
 PC_STA_INFO          : 0
 PC_NEIGH_INFO        : 0
 PC_LOW_RSSI          : 0
 PC_TEMP_DISCONN      : 0
 PC_AP_FAILURE        : 0
 PC_UNKNOWN_AP        : 0
```

# show wireless statistics mobility

To see the wireless mobility manager statistics, use the **show wireless stats mobility** command.

**show wireless stats mobility** {**dtls** | **messages**} [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

## Syntax Description

| | |
|---|---|
| **dtls** | View the mobility dtls messages statistics. |
| **messages** | View the mobility messages statistics. |
| *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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see the statistics of the wireless mobiliy manager:

```
Device# show wireless stats mobility
```

# show wireless stats mesh packet error

To see the packet statistics of all connected mesh APs, use the **show wireless stats mesh packet error** command.

**show wireless stats mesh packet error** [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

## Syntax Description

| | |
|---|---|
| **packet** | Shows packet statistics information. |
| **error** | Shows packet statistics of all connected mesh APs. |
| **active R0** | Active instance of the active AP filters in Route-processor slot 0. |
| **standby R0** | Standby instance of the active AP filters in Route-processor slot 0. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see the packet error statistics of all connected mesh APs:

```
Device# show wireless stats mesh packet error
```

# show wireless stats mesh security and queue

To see the mesh queue and security statistics of all connected mesh APs, use the **show wireless stats mesh** command.

**show wireless stats mesh** {**security** | **queue**} [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

## Syntax Description

| | |
|---|---|
| **queue** | Shows queue statistics of all connected mesh APs. |
| **security** | Shows security statistics of all connected mesh APs. |
| *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

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see the security statistics of all connected mesh APs:

```
Device# show wireless stats mesh security
```

# show wireless stats redundancy config database

To view the high availabilty redundancy configuration statistics, use the **show wireless stats redundancy config database** command.

**show wireless stats redundancy config database** { **mobility** | **nmspd** | **rrm** | **wncd** | **wncmgrd** } *instance-id* **chassis** { *chassis-num* | **active** | **standby** } **R0**

## Syntax Description

| | |
|---|---|
| **mobility** | Specifes the statistics of Mobilityd configuration database. |
| **nmspd** | Specifes the statistics of NMSPD configuration database. |
| **rrm** | Specifes the statistics of RRM configuration database. |
| **wncd** | Specifes the statistics of WNCD configuration database. |
| **wncmgrd** | Specifes the statistics of WNCD configuration database. |
| *instance-id* | Instance ID. Valid values range from 0 to 7. |
| **chassis** | Specifies the chassis. |
| *chassis-num* | Chassis number. |
| **active** | Specifies the active instance. |
| **standby** | Specifies the standby instance. |
| **R0** | Specifies the route processor slot. |

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Cupertino 17.7.1 | This command was introduced. |

## Examples

The following example shows how to view the high availabilty redundancy configuration statistics:

```
Device# show wireless stats redundancy config database wncd 0 chassis 1 R0

Wncd Configuration Sync Statistics
 Index   Number of Locks    Duration(sec)   Threshold-count   Max-Duration(nsec)
--------------------------------------------------------------------------------
    1       535               127              1           1112156700
```

# show wireless summary

To display the number of access points, radios and wireless clients known to the controller, use the **show wireless summary** command in privileged EXEC mode.

**show wireless summary**

### Syntax Description

This command has no arguments or keywords.

### Command Default

No default behavior or values.

### Command Modes

Privileged EXEC

### Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

The following is sample output from the **show wireless summary** command:

```
Device# show wireless summary

Access Point Summary

               Total    Up    Down
-----------------------------------
802.11a/n          2     2       0
802.11b/g/n        2     2       0
All APs            2     2       0

Client Summary

Current Clients : 1
Excluded Clients: 0
Disabled Clients: 0
```

# show wireless urlfilter details

To view the details of a specified wireless URL filter, use the **show wireless urlfilter details** command.

**show wireless urlfilter details** *list-name*

## Syntax Description

This command has no arguments.

## Command Default

None

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the details of a specified wireless URL filter:

```
Device# show wireless urlfilter details urllist_flex_preauth
List Name................. : urllist_flex_preauth
Filter ID.............. : : 1
Filter Type.............. : PRE-AUTH
Action.................... : PERMIT
Redirect server ipv4...... : 8.8.8.8
Redirect server ipv6...... : 2001:0300:0008:0000:0000:0000:0000:0081
Configured List of URLs
   URL.................... : url1.dns.com
```

# show wireless urlfilter summary

To view the summary of all wireless URL filters, use the **show wireless urlfilter summary** command.

**show wireless urlfilter summary**

## Syntax Description

This command has no arguments.

## Command Default

None

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

This example shows how to view the summary of all wireless URL filters:

```
Device# show wireless urlfilter summary
Black-list    - DENY
White-list    - PERMIT
Filter-Type   - Specific to Local Mode

URL-List                         ID  Filter-Type  Action   Redirect-ipv4  Redirect-ipv6
------------------------------------------------------------------------------------------
urllist_flex_preauth             1    PRE-AUTH     PERMIT    8.8.8.8
2001:0300:0008:0000:0000:0000:0000:0081
```

# show wireless vlan details

To see the VLAN details, use the **show wireless vlan details** command.

**show wireless vlan details** [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see the VLAN details:

```
Device# show wireless vlan details chassis active r0
```

# show wireless wgb mac-address

To view all the clients of the wireless workgroup bridge (WGB) using its MAC address, use the **show wireless wgb mac-address** command.

**show wireless wgb mac-address** *mac-address* **detail**

## Syntax Description

| | |
|---|---|
| *mac-address* | MAC address of the WGB. |
| **detail** | View clients of the wireless WGB. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see the clients of the wireless WGB:

```
Device# show wireless wgb mac-address 98-C7-7B-09-EF-ED detail
```

# show wireless wgb summary

To see the active workgroup bridges (WGB), use the **show wireless wgb summary** command.

**show wireless wgb summary**

### Command Default

None

### Command Modes

Privileged EXEC

### Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see the active workgroup bridges (WGB):

```
Device# show wireless wgb summary
```

# show wireless wps rogue

To see the Rogue AP and Client information, use the **show wireless wps rogue** command.

**See Adhoc Rogues (IBSS) information**
**show wireless wps rogue** {**adhoc** | {**detailed***mac-addr*} | **summary**}

**See rogue AP information**
**show wireless wps rogueap** {**clients***mac-addr* | **customsummary** | **detailed***mac-addr* | **friendlysummary** | **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**]

## Syntax Description

| | |
|---|---|
| *mac-address* | MAC address of the client. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced in a release earlier than Cisco IOS XE Gibraltar 16.10.1. |

### Examples

The following example shows how to see the rogue feature statistics:

```
Device# show wireless wps rogue stats
```

# show wireless wps rogue ap summary

To display a list of all rogue access points detected by the device, use the **show wireless wps rogue ap summary** command.

**show wireless wps rogue ap summary**

## Command Default

None.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| | This command was introduced. |

## Usage Guidelines

None.

This example shows how to display a list of all rogue access points detected by the device:

```
Device# show wireless wps rogue ap summary
Rogue Location Discovery Protocol           : Disabled
Rogue on wire Auto-Contain                  : Disabled
Rogue using our SSID Auto-Contain           : Disabled
Valid client on rogue AP Auto-Contain       : Disabled
Rogue AP timeout                            : 1200
Rogue Detection Report Interval             : 10
Rogue AP minimum RSSI                       : -128
Rogue AP minimum transient time             : 0

Number of rogue APs detected : 624

MAC Address         Classification     # APs    # Clients   Last Heard
--------------------------------------------------------------------------------------
0018.e78d.250a      Unclassified       1        0           Thu Jul 25 05:04:01 2013
0019.0705.d5bc      Unclassified       1        0           Thu Jul 25 05:16:26 2013
0019.0705.d5bd      Unclassified       1        0           Thu Jul 25 05:10:28 2013
0019.0705.d5bf      Unclassified       1        0           Thu Jul 25 05:16:26 2013
```

# show wireless wps rogue client detailed

To view the detailed information of a specific rogue client, use the **show wireless wps rogue client detailed** *client-mac* command.

**show wireless wps rogue client detailed** *client-mac*

## Syntax Description

| | |
|---|---|
| *client-mac* | MAC address of the rogue client. |

## Command Default

None.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

None.

This example shows how to display the detailed information for a specific rogue client:

```
Device# show wireless wps rogue client detail  0024.d7f1.2558
Rogue BSSID                          : 64d8.146f.379f
Rogue Radio Type                     : 802.11n - 5GHz
State                                : Alert
First Time Rogue was Reported        : Wed Aug  7 12:51:43 2013
Last Time Rogue was Reported         : Wed Aug  7 12:51:43 2013
Reported by
  AP 2
    MAC Address                      : 3cce.7309.0370
    Name                             : AP3502-talwar-ccie
    Radio Type                       : 802.11a
    RSSI                             : -42 dBm
    SNR                              : 47 dB
    Channel                          : 52
    Last reported by this AP         : Wed Aug  7 12:51:43 2013
```

# show wireless wps rogue ap detailed

To view the detailed information of a rogue access point, use **show wireless wps rogue ap detailed** *mac-address* command.

**show wireless wps rogue ap detailed** *0008.30a7.7797*

## Syntax Description

| | |
|---|---|
| *mac-address* | The MAC address of the rogue access point.<br>**Note** If a rogue access point uses dot11n on 2.4GHz, the command output displays the **radio type** as **dot11g , dot11n - 2.4 GHz**. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Fuji 16.7.x | This command was introduced. |

### Example

This example shows how to display the detailed information about a rogue access point:

```
Device# wireless wps rogue ap detailed 0008.30a7.7797
Rogue Event history

Rogue BSSID                              : 0008.30a7.7797
Is Rogue on Wired Network                : No
Classification                           : Unclassified
Manually Contained                       : Yes
State                                    : Contained Pending
Containment Level                        : 1
Number of Containing APs                 : 0
First Time Rogue was Reported            : 03/08/2017 17:41:55
Last Time Rogue was Reported             : 03/08/2017 21:48:34

Number of clients                        : 0

Reported By
  AP Name : JEWLC-AA
    MAC Address                          : 00d7.8f4e.7240
    Detecting slot ID                    : 0
    Radio Type                           : dot11g , dot11n - 2.4 GHz
    SSID                                 : psk
    Channel                              : 5
    Channel Width                        : 20 MHz
    RSSI                                 : -128 dBm
    SNR                                  : 0 dB
    Encryption                           : Enabled
    ShortPreamble                        : Disabled
    WPA Support                          : Not Friendly
    Last reported by this AP             : 03/08/2017 21:48:34
```

# show wireless wps rogue client summary

To display summary of WPS rogue clients, use the **show wireless wps rogue client summary** command.

**show wireless wps rogue client summary**

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |

## Usage Guidelines

### Example

The following displays the output of the **show wireless wps rogue client summary** command:

```
Device# show wireless wps rogue client summary
Validate rogue clients against AAA  : Disabled
Validate rogue clients against MSE  : Enabled
Number of rogue clients detected : 0
```

# show wps summary

To display Wireless Protection System (WPS) summary information, use the **show wps summary** command.

**show wps summary**

## 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
...
```

# shutdown

To close the RF Profile and disable the network, use the **shutdown** command. To disable shutdown execution, use the **no** form of this command.

**shutdown**

## Syntax Description

| | |
|---|---|
| **shutdown** | Shuts down the profile and disables network. |

## Command Default

None

## Command Modes

config-rf-profile

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Denali 16.3.1 | This command was introduced. |

## Usage Guidelines

None

This example shows how to close a RF Profile and disable the network.

```
Device(config-rf-profile)#shutdown
```

# INDEX