



# Security

---

- [aaa accounting, on page 4](#)
- [aaa accounting dot1x, on page 7](#)
- [aaa accounting identity, on page 9](#)
- [aaa authentication dot1x, on page 11](#)
- [aaa new-model, on page 12](#)
- [authentication host-mode, on page 14](#)
- [authentication logging verbose, on page 16](#)
- [authentication mac-move permit, on page 17](#)
- [authentication priority, on page 19](#)
- [authentication violation, on page 21](#)
- [cisp enable, on page 23](#)
- [clear errdisable interface vlan, on page 24](#)
- [clear mac address-table, on page 25](#)
- [confidentiality-offset, on page 27](#)
- [delay-protection, on page 28](#)
- [deny \(MAC access-list configuration\), on page 29](#)
- [device-role \(IPv6 snooping\), on page 32](#)
- [device-role \(IPv6 nd inspection\), on page 33](#)
- [device-tracking policy, on page 34](#)
- [dot1x critical \(global configuration\), on page 36](#)
- [dot1x logging verbose, on page 37](#)
- [dot1x pae, on page 38](#)
- [dot1x supplicant controlled transient, on page 39](#)
- [dot1x supplicant force-multicast, on page 40](#)
- [dot1x test eapol-capable, on page 41](#)
- [dot1x test timeout, on page 42](#)
- [dot1x timeout, on page 43](#)
- [dtls, on page 45](#)
- [enable password, on page 47](#)
- [enable secret, on page 49](#)
- [epm access-control open, on page 52](#)
- [include-icv-indicator, on page 53](#)
- [ip access-list, on page 54](#)

- [ip access-list role-based](#), on page 57
- [ip admission](#), on page 58
- [ip admission name](#), on page 59
- [ip dhcp snooping database](#), on page 61
- [ip dhcp snooping information option format remote-id](#), on page 63
- [ip dhcp snooping verify no-relay-agent-address](#), on page 64
- [ip http access-class](#), on page 65
- [ip radius source-interface](#), on page 67
- [ip source binding](#), on page 69
- [ip ssh source-interface](#), on page 70
- [ip verify source](#), on page 71
- [ipv6 access-list](#), on page 72
- [ipv6 snooping policy](#), on page 74
- [key chain macsec](#), on page 75
- [key config-key password-encrypt](#), on page 76
- [key-server](#), on page 78
- [limit address-count](#), on page 79
- [mab logging verbose](#), on page 80
- [mab request format attribute 32](#), on page 81
- [macsec-cipher-suite](#), on page 83
- [macsec network-link](#), on page 85
- [match \(access-map configuration\)](#), on page 86
- [mka pre-shared-key](#), on page 88
- [mka suppress syslogs sak-rekey](#), on page 89
- [password encryption aes](#), on page 90
- [permit \(MAC access-list configuration\)](#), on page 92
- [protocol \(IPv6 snooping\)](#), on page 95
- [radius server](#), on page 96
- [sak-rekey](#), on page 98
- [security level \(IPv6 snooping\)](#), on page 99
- [send-secure-announcements](#), on page 100
- [server-private \(RADIUS\)](#), on page 101
- [server-private \(TACACS+\)](#), on page 103
- [show aaa clients](#), on page 105
- [show aaa command handler](#), on page 106
- [show aaa local](#), on page 107
- [show aaa servers](#), on page 109
- [show aaa sessions](#), on page 110
- [show authentication brief](#), on page 111
- [show authentication sessions](#), on page 114
- [show cisp](#), on page 117
- [show dot1x](#), on page 119
- [show eap pac peer](#), on page 121
- [show ip access-lists](#), on page 122
- [show ip dhcp snooping statistics](#), on page 125
- [show radius server-group](#), on page 128

- [show tech-support acl](#), on page 130
- [show tech-support identity](#), on page 134
- [show vlan access-map](#), on page 143
- [show vlan filter](#), on page 144
- [show vlan group](#), on page 145
- [switchport port-security aging](#), on page 146
- [switchport port-security mac-address](#), on page 148
- [switchport port-security maximum](#), on page 151
- [switchport port-security violation](#), on page 153
- [tacacs server](#), on page 155
- [tracking \(IPv6 snooping\)](#), on page 156
- [trusted-port](#), on page 158
- [username](#), on page 159
- [vlan access-map](#), on page 164
- [vlan dot1Q tag native](#), on page 166
- [vlan filter](#), on page 167
- [vlan group](#), on page 168

## aaa accounting

To enable authentication, authorization, and accounting (AAA) accounting of requested services for billing or security purposes when you use RADIUS or TACACS+, use the **aaa accounting** command in global configuration mode. To disable AAA accounting, use the **no** form of this command.

```
aaa accounting {auth-proxy | system | network | exec | connections | commands level}
{default | list-name} {start-stop | stop-only | none} [broadcast] group group-name
no aaa accounting {auth-proxy | system | network | exec | connections | commands level}
{default | list-name} {start-stop | stop-only | none} [broadcast] group group-name
```

### Syntax Description

|                                  |   |
|----------------------------------|---|
| <b>auth-proxy</b>                | Provides information about all authenticated-proxy user events.   |
| <b>system</b>                    | Performs accounting for all system-level events not associated with users, such as reloads.   |
| <b>network</b>                   | Runs accounting for all network-related service requests.   |
| <b>exec</b>                      | Runs accounting for EXEC shell session. This keyword might return user profile information such as what is generated by the <b>autocommand</b> command.   |
| <b>connection</b>                | Provides information about all outbound connections made from the network access server.  |
| <b>commands level</b>            | Runs accounting for all commands at the specified privilege level. Valid privilege level entries are integers from 0 through 15.  |
| <b>default</b>                   | Uses the listed accounting methods that follow this argument as the default list of methods for accounting services.  |
| <i>list-name</i>                 | Character string used to name the list of at least one of the accounting methods described in   |
| <b>start-stop</b>                | 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 the "start" accounting notice was received by the accounting server. |
| <b>stop-only</b>                 | Sends a "stop" accounting notice at the end of the requested user process.  |
| <b>none</b>                      | Disables accounting services on this line or interface.   |
| <b>broadcast</b>                 | (Optional) Enables sending accounting records to multiple AAA servers. Simultaneously sends accounting records to the first server in each group. If the first server is unavailable, fail over occurs using the backup servers defined within that group.  |
| <i>group</i><br><i>groupname</i> | At least one of the keywords described in the AAA Accounting Methods table.   |

### Command Default

AAA accounting is disabled.

### Command Modes

Global configuration (config)

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

**Usage Guidelines** Use the **aaa accounting** command to enable accounting and to create named method lists defining specific accounting methods on a per-line or per-interface basis.

**Table 1: AAA Accounting Methods**

| Keyword                 | Description  |
|-------------------------|--|
| <b>group radius</b>     | Uses the list of all RADIUS servers for authentication as defined by the <b>aaa group server radius</b> command.   |
| <b>group tacacs+</b>    | Uses the list of all TACACS+ servers for authentication as defined by the <b>aaa group server tacacs+</b> command. |
| <b>group group-name</b> | Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the server group group-name.               |

In AAA Accounting Methods table, the **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** and **aaa group server tacacs+** commands to create a named group of servers.

Cisco IOS XE software supports the following two methods of accounting:

- **RADIUS**—The network access server reports user activity to the RADIUS security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server.
- **TACACS+**—The network access server reports user activity to the TACACS+ security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server.

Method lists for accounting define the way accounting will be performed. Named accounting method lists enable you to designate a particular security protocol to be used on specific lines or interfaces for particular types of accounting services. Create a list by entering the *list-name* and the *method*, where *list-name* is any character string used to name this list (excluding the names of methods, such as radius or tacacs+) and *method* identifies the methods to be tried in sequence as given.

If the **aaa accounting** command for a particular accounting type is issued without a named method list specified, the default method list is automatically applied to all interfaces or lines (where this accounting 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 accounting takes place.



**Note** System accounting does not use named accounting lists; you can only define the default list for system accounting.

For minimal accounting, include the **stop-only** keyword to send a stop record accounting notice at the end of the requested user process. For more accounting, you can include the **start-stop** keyword, so that RADIUS or TACACS+ sends a start accounting notice at the beginning of the requested process and a stop accounting

notice at the end of the process. Accounting is stored only on the RADIUS or TACACS+ server. The `none` keyword disables accounting services for the specified line or interface.

When AAA accounting is activated, the network access server monitors either RADIUS accounting attributes or TACACS+ AV pairs pertinent to the connection, depending on the security method you have implemented. The network access server reports these attributes as accounting records, which are then stored in an accounting log on the security server.



---

**Note** This command cannot be used with TACACS or extended TACACS.

---

This example defines a default commands accounting method list, where accounting services are provided by a TACACS+ security server, set for privilege level 15 commands with a stop-only restriction:

```
Device> enable
Device# configure terminal
Device(config)# aaa accounting commands 15 default stop-only group TACACS+
Device(config)# exit
```

This example defines a default auth-proxy accounting method list, where accounting services are provided by a TACACS+ security server with a stop-only restriction. The **aaa accounting** commands activates authentication proxy accounting.

```
Device> enable
Device# configure terminal
Device(config)# aaa new model
Device(config)# aaa authentication login default group TACACS+
Device(config)# aaa authorization auth-proxy default group TACACS+
Device(config)# aaa accounting auth-proxy default start-stop group TACACS+
Device(config)# exit
```

## aaa accounting dot1x

To enable authentication, authorization, and accounting (AAA) accounting and to create method lists defining specific accounting methods on a per-line or per-interface basis for IEEE 802.1x sessions, use the **aaa accounting dot1x** command in global configuration mode. To disable IEEE 802.1x accounting, use the **no** form of this command.

```
aaa accounting dot1x {name | default} start-stop {broadcast group {name | radius | tacacs+}
[group {name | radius | tacacs+} ... ] | group {name | radius | tacacs+} [group
{name | radius | tacacs+} ... ]}
no aaa accounting dot1x {name | default}
```

### Syntax Description

|                   |   |
|-------------------|---|
| <i>name</i>       | Name of a server group. This is optional when you enter it after the <b>broadcast group</b> and <b>group</b> keywords.  |
| <b>default</b>    | Specifies the accounting methods that follow as the default list for accounting services.   |
| <b>start-stop</b> | 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.  |
| <b>broadcast</b>  | Enables accounting records to be sent to multiple AAA servers and sends 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.  |
| <b>group</b>      | Specifies the server group to be used for accounting services. These are valid server group names: <ul style="list-style-type: none"> <li>• <i>name</i> — Name of a server group.</li> <li>• <b>radius</b> — Lists of all RADIUS hosts.</li> <li>• <b>tacacs+</b> — Lists of all TACACS+ hosts.</li> </ul> <p>The <b>group</b> keyword is optional when you enter it after the <b>broadcast group</b> and <b>group</b> keywords. You can enter more than optional <b>group</b> keyword.</p> |
| <b>radius</b>     | (Optional) Enables RADIUS accounting.   |
| <b>tacacs+</b>    | (Optional) Enables TACACS+ accounting.  |

### Command Default

AAA accounting is disabled.

### Command Modes

Global configuration (config)

### Command History

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

---

**Usage Guidelines**

This command requires access to a RADIUS server.

We recommend that you enter the **dot1x reauthentication** interface configuration command before configuring IEEE 802.1x RADIUS accounting on an interface.

This example shows how to configure IEEE 802.1x accounting:

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa accounting dot1x default start-stop group radius
Device(config)# exit
```



## aaa accounting identity

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

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

|                    |  |   |
|--------------------|--|---|
| Syntax Description | <b>name</b>  | Name of a server group. This is optional when you enter it after the <b>broadcast group</b> and <b>group</b> keywords.  |
|                    | <b>default</b>   | Uses the accounting methods that follow as the default list for accounting services.  |
|                    | <b>start-stop</b>  | 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.  |
|                    | <b>broadcast</b>   | Enables accounting records to be sent to multiple AAA servers and send accounting records to the first server in each group. If the first server is unavailable, the switch uses the list of backup servers to identify the first server.   |
|                    | <b>group</b>   | Specifies the server group to be used for accounting services. These are valid server group names: <ul style="list-style-type: none"> <li>• <b>name</b> — Name of a server group.</li> <li>• <b>radius</b> — Lists of all RADIUS hosts.</li> <li>• <b>tacacs+</b> — Lists of all TACACS+ hosts.</li> </ul> <p>The <b>group</b> keyword is optional when you enter it after the <b>broadcast group</b> and <b>group</b> keywords. You can enter more than optional <b>group</b> keyword.</p> |
|                    | <b>radius</b>  | (Optional) Enables RADIUS authorization.  |
|                    | <b>tacacs+</b>   | (Optional) Enables TACACS+ accounting.  |
|                    |  |   |
| Command Default    | AAA accounting is disabled.  |   |
| Command Modes      | Global configuration (config)  |   |
| Command History    | <b>Release</b>   | <b>Modification</b>   |
|                    | Cisco IOS XE Everest 16.6.1  | This command was introduced.  |
| Usage Guidelines   | To enable AAA accounting identity, you need to enable policy mode. To enable policy mode, enter the <b>authentication display new-style</b> 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
```

```
Device(config)# exit
```

## 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 <b>group radius</b> keywords to use the list of all RADIUS servers for authentication.       |  |
|                    | Note                            | Though other keywords are visible in the command-line help strings, only the <b>default</b> and <b>group radius</b> keywords are supported. |  |
|                    |                                 |   |  |
| Command Default    | No authentication is performed. |   |  |
| Command Modes      | Global configuration (config)   |   |  |
| Command History    | Release                         | Modification  |  |
|                    | Cisco IOS XE Everest 16.6.1     | 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> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication dot1x default group radius
Device(config)# exit
```

# 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 Everest 16.6.1 | 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 switch to get the default configuration or the **login** command. If the switch is not reloaded, the switch defaults to the **login local** command under the VTY.



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

## Examples

The following example initializes AAA:

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# exit
```

The following example shows a VTY configured and the **aaa new-model** command removed:

```
Device> enable
Device# configure terminal
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
```

!

**Related Commands**

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

# authentication host-mode

To set the authorization manager mode on a port, use the **authentication host-mode** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

**authentication host-mode** {**multi-auth** | **multi-domain** | **multi-host** | **single-host**}  
**no authentication host-mode**

|                    |  |  |
|--------------------|--|--|
| Syntax Description | multi-auth   | Enables multiple-authorization mode (multi-auth mode) on the port. |
|                    | multi-domain   | Enables multiple-domain mode on the port.                          |
|                    | multi-host   | Enables multiple-host mode on the port.                            |
|                    | single-host  | Enables single-host mode on the port.                              |
| Command Default    | Single host mode is enabled.   |  |
| Command Modes      | Interface configuration (config-if)  |  |
| Command History    | Release  | Modification   |
|                    | Cisco IOS XE Everest 16.6.1  | This command was introduced.                                       |
| Usage Guidelines   | Single-host mode should be configured if only one data host is connected. Do not connect a voice device to authenticate on a single-host port. Voice device authorization fails if no voice VLAN is configured on the port.                                |  |
|                    | Multi-domain mode should be configured if data host is connected through an IP phone to the port. Multi-domain mode should be configured if the voice device needs to be authenticated.  |  |
|                    | Multi-auth mode should be configured to allow devices behind a hub to obtain secured port access through individual authentication. Only one voice device can be authenticated in this mode if a voice VLAN is configured.                                 |  |
|                    | Multi-host mode also offers port access for multiple hosts behind a hub, but multi-host mode gives unrestricted port access to the devices after the first user gets authenticated.  |  |
|                    | This example shows how to enable multi-auth mode on a port:<br><br>Device> enable<br>Device# configure terminal<br>Device(config)# interface gigabitethernet 2/0/1<br>Device(config-if)# authentication host-mode multi-auth<br>Device(config-if)# end     |  |
|                    | This example shows how to enable multi-domain mode on a port:<br><br>Device> enable<br>Device# configure terminal<br>Device(config)# interface gigabitethernet 2/0/1<br>Device(config-if)# authentication host-mode multi-domain<br>Device(config-if)# end |  |

This example shows how to enable multi-host mode on a port:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 2/0/1
Device(config-if)# authentication host-mode multi-host
Device(config-if)# end
```

This example shows how to enable single-host mode on a port:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 2/0/1
Device(config-if)# authentication host-mode single-host
Device(config-if)# end
```

You can verify your settings by entering the **show authentication sessions interface** *interface details* privileged EXEC command.

# authentication logging verbose

To filter detailed information from authentication system messages, use the **authentication logging verbose** command in global configuration mode on the switch stack or on a standalone switch.

**authentication logging verbose**  
**no authentication logging verbose**

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

**Command Default** Detailed logging of system messages is not enabled.

**Command Modes** Global configuration (config)

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

**Usage Guidelines** This command filters details, such as anticipated success, from authentication system messages. Failure messages are not filtered.

To filter verbose authentication system messages:

```
Device> enable
Device# configure terminal
Device(config)# authentication logging verbose
Device(config)# exit
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

| Related Commands | Command                               | Description  |
|------------------|---------------------------------------|--|
|                  | <b>authentication logging verbose</b> | Filters details from authentication system messages.       |
|                  | <b>dot1x logging verbose</b>          | Filters details from dot1x authentication system messages. |
|                  | <b>mab logging verbose</b>            | Filters details from MAB authentication system messages.   |



# authentication mac-move permit

To enable MAC move on a device, use the **authentication mac-move permit** command in global configuration mode. To disable MAC move, use the **no** form of this command.

**authentication mac-move permit**  
**no authentication mac-move permit**

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

**Command Default** MAC move is disabled.

**Command Modes** Global configuration (config)

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

**Usage Guidelines** The command enables authenticated hosts to move between any authentication-enabled ports (MAC authentication bypass [MAB], 802.1x, or Web-auth) on a device. For example, if there is a device between an authenticated host and port, and that host moves to another port, the authentication session is deleted from the first port, and the host is reauthenticated on the new port.

If MAC move is disabled, and an authenticated host moves to another port, it is not reauthenticated, and a violation error occurs.

This example shows how to enable MAC move on a device:

```
Device> enable
Device# configure terminal
Device(config)# authentication mac-move permit
Device(config)# exit
```

| Related Commands | Command                             | Description  |
|------------------|-------------------------------------|--|
|                  | <b>access-session mac-move deny</b> | Disables MAC move on a device.   |
|                  | <b>authentication event</b>         | Sets the action for specific authentication events.                          |
|                  | <b>authentication fallback</b>      | Configures a port to use web authentication as a IEEE 802.1x authentication. |
|                  | <b>authentication host-mode</b>     | Sets the authorization manager mode on a port.                               |
|                  | <b>authentication open</b>          | Enables or disables open access on a port.                                   |
|                  | <b>authentication order</b>         | Sets the order of authentication methods used on a port.                     |
|                  | <b>authentication periodic</b>      | Enable or disables reauthentication on a port.                               |
|                  | <b>authentication port-control</b>  | Enables manual control of the port authorization.                            |

| Command                         | Description   |
|---------------------------------|---|
| <b>authentication priority</b>  | Adds an authentication method to the port-priority list.  |
| <b>authentication timer</b>     | Configures the timeout and reauthentication parameters.   |
| <b>authentication violation</b> | Configures the violation modes that occur when a network device connects to a port with the maximum number of violations. |
| <b>show authentication</b>      | Displays information about authentication manager.  |

# authentication priority

To add an authentication method to the port-priority list, use the **authentication priority** command in interface configuration mode. To return to the default, use the **no** form of this command.

**authentication priority** [**dot1x** | **mab**] {**webauth**}  
**no authentication priority** [**dot1x** | **mab**] {**webauth**}

| Syntax Description | <b>dot1x</b>   | (Optional) Adds 802.1x to the order of authentication methods.                          |
|--------------------|----------------|---|
|                    | <b>mab</b>     | (Optional) Adds MAC authentication bypass (MAB) to the order of authentication methods. |
|                    | <b>webauth</b> | Adds web authentication to the order of authentication methods.                         |

|                        |  |
|------------------------|--|
| <b>Command Default</b> | The default priority is 802.1x authentication, followed by MAC authentication bypass and web authentication. |
|------------------------|--|

|                      |                                     |
|----------------------|-------------------------------------|
| <b>Command Modes</b> | Interface configuration (config-if) |
|----------------------|-------------------------------------|

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

**Usage Guidelines**

Ordering sets the order of methods that the device attempts when trying to authenticate a new device is connected to a port.

When configuring multiple fallback methods on a port, set web authentication (webauth) last.

Assigning priorities to different authentication methods allows a higher-priority method to interrupt an in-progress authentication method with a lower priority.



**Note** If a client is already authenticated, it might be reauthenticated if an interruption from a higher-priority method occurs.

The default priority of an authentication method is equivalent to its position in execution-list order: 802.1x authentication, MAC authentication bypass (MAB), and web authentication. Use the **dot1x**, **mab**, and **webauth** keywords to change this default order.

This example shows how to set 802.1x as the first authentication method and web authentication as the second authentication method:

```
Device(config-if)# authentication priority dot1x webauth
```

This example shows how to set MAB as the first authentication method and web authentication as the second authentication method:

```
Device> enable
Device# configure terminal
```

```

Device(config)# interface gigabitethernet 0/1/2
Device(config-if)# authentication priority mab webauth
Device(config-if)# end

```

**Related Commands**

| Command  | Description  |
|--|--|
| <b>authentication control-direction</b>                      | Configures the port mode as unidirectional or bidirectional.   |
| <b>authentication event fail</b>                             | Specifies how the Auth Manager handles authentication failures as a result of a failed authentication attempt.                 |
| <b>authentication event no-response action</b>               | Specifies how the Auth Manager handles authentication failures as a result of no response from the server.                     |
| <b>authentication event server alive action reinitialize</b> | Reinitializes an authorized Auth Manager session when a previously authorized session and accounting server becomes available. |
| <b>authentication event server dead action authorize</b>     | Authorizes Auth Manager sessions when the authentication, authorization, and accounting server becomes unreachable.            |
| <b>authentication fallback</b>                               | Enables a web authentication fallback method.  |
| <b>authentication host-mode</b>                              | Allows hosts to gain access to a controlled port.  |
| <b>authentication open</b>                                   | Enables open access on a port.   |
| <b>authentication order</b>                                  | Specifies the order in which the Auth Manager attempts to authenticate a user.   |
| <b>authentication periodic</b>                               | Enables automatic reauthentication on a port.  |
| <b>authentication port-control</b>                           | Configures the authorization state of a controlled port.   |
| <b>authentication timer inactivity</b>                       | Configures the time after which an inactive Auth Manager session is terminated.  |
| <b>authentication timer reauthenticate</b>                   | Specifies the period of time between which the Auth Manager attempts to reauthenticate a user.                                 |
| <b>authentication timer restart</b>                          | Specifies the period of time after which the Auth Manager attempts to restart a session.                                       |
| <b>authentication violation</b>                              | Specifies the action to be taken when a security violation occurs on a port.   |
| <b>mab</b>   | Enables MAC authentication bypass on a port.   |
| <b>show authentication registrations</b>                     | Displays information about the authentication methods that are registered on a port.   |
| <b>show authentication sessions</b>                          | Displays information about current Auth Manager sessions.  |
| <b>show authentication sessions interface</b>                | Displays information about the Auth Manager for a given interface.   |

# authentication violation

To configure the violation modes that occur when a new device connects to a port or when a new device connects to a port after the maximum number of devices are connected to that port, use the **authentication violation** command in interface configuration mode.

```
authentication violation { protect | replace | restrict | shutdown }
no authentication violation { protect | replace | restrict | shutdown }
```

|                    |                 |  |
|--------------------|-----------------|--|
| Syntax Description | <b>protect</b>  | Drops unexpected incoming MAC addresses. No syslog errors are generated.               |
|                    | <b>replace</b>  | Removes the current session and initiates authentication with the new host.            |
|                    | <b>restrict</b> | Generates a syslog error when a violation error occurs.                                |
|                    | <b>shutdown</b> | Error-disables the port or the virtual port on which an unexpected MAC address occurs. |

**Command Default** Authentication violation shutdown mode is enabled.

**Command Modes** Interface configuration (config-if)

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

**Usage Guidelines** Use the **authentication violation** command to specify the action to be taken when a security violation occurs on a port.

This example shows how to configure an IEEE 802.1x-enabled port as error-disabled and to shut down when a new device connects it:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 2/0/1
Device(config-if)# authentication violation shutdown
Device(config-if)# end
```

This example shows how to configure an 802.1x-enabled port to generate a system error message and to change the port to restricted mode when a new device connects to it:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 2/0/1
Device(config-if)# authentication violation restrict
Device(config-if)# end
```

This example shows how to configure an 802.1x-enabled port to ignore a new device when it connects to the port:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 2/0/1
Device(config-if)# authentication violation protect
Device(config-if)# end
```

This example shows how to configure an 802.1x-enabled port to remove the current session and initiate authentication with a new device when it connects to the port:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 2/0/1
Device(config-if)# authentication violation replace
Device(config-if)# end
```

You can verify your settings by entering the **show authentication** command.

# cisp enable

To enable Client Information Signaling Protocol (CISP) on a device so that it acts as an authenticator to a supplicant device and a supplicant to an authenticator device, use the **cisp enable** global configuration command.

**cisp enable**  
**no cisp enable**

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> | This command has no arguments or keywords. |
|---------------------------|--|

|                        |                                |
|------------------------|--------------------------------|
| <b>Command Default</b> | No default behavior or values. |
|------------------------|--------------------------------|

|                      |                               |
|----------------------|-------------------------------|
| <b>Command Modes</b> | Global configuration (config) |
|----------------------|-------------------------------|

| <b>Command History</b> | <b>Release</b>              | <b>Modification</b>          |
|------------------------|-----------------------------|------------------------------|
|                        | Cisco IOS XE Everest 16.6.1 | This command was introduced. |

|                         |  |
|-------------------------|--|
| <b>Usage Guidelines</b> | The link between the authenticator and supplicant device is a trunk. When you enable VTP on both devices, the VTP domain name must be the same, and the VTP mode must be server. |
|-------------------------|--|

To avoid the MD5 checksum mismatch error when you configure VTP mode, verify that:

- VLANs are not configured on two different devices, which can be caused by two VTP servers in the same domain.
- Both devices have different configuration revision numbers.

This example shows how to enable CISP:

```
Device> enable
Device# configure terminal
Device(config)# cisp enable
Device(config)# exit
```

| Related Commands | Command                                      | Description  |
|------------------|--|--|
|                  | <b>dot1x credentialsprofile</b>              | Configures a profile on a supplicant device.         |
|                  | <b>dot1x supplicant force-multicast</b>      | Forces 802.1X supplicant to send multicast packets.  |
|                  | <b>dot1x supplicant controlled transient</b> | Configures controlled access by 802.1X supplicant.   |
|                  | <b>show cisp</b>                             | Displays CISP information for a specified interface. |

# clear errdisable interface vlan

To reenable a VLAN that was error-disabled, use the **clear errdisable interface** command in privileged EXEC mode.

**clear errdisable interface** *interface-id* **vlan** [*vlan-list*]

|                           |                     |  |
|---------------------------|---------------------|--|
| <b>Syntax Description</b> | <i>interface-id</i> | Specifies an interface.                                      |
|                           | <i>vlan list</i>    | (Optional) Specifies a list of VLANs to be reenabled. If a V |

**Command Default** No default behavior or values.

**Command Modes** Privileged EXEC (#)

|                        |                             |                              |
|------------------------|-----------------------------|------------------------------|
| <b>Command History</b> | <b>Release</b>              | <b>Modification</b>          |
|                        | Cisco IOS XE Everest 16.6.1 | This command was introduced. |

**Usage Guidelines** You can reenable a port by using the **shutdown** and **no shutdown** interface configuration commands, or you can clear error-disable for VLANs by using the **clear errdisable interface** command.

**Examples** This example shows how to reenable all VLANs that were error-disabled on Gigabit Ethernet port 4/0/2:

```
Device# clear errdisable interface gigabitethernet4/0/2 vlan
```

|                         |  |                                       |
|-------------------------|--|---------------------------------------|
| <b>Related Commands</b> | <b>Command</b>                             | <b>Description</b>                    |
|                         | <b>errdisable detect cause</b>             | Enables error-disabled detection fo   |
|                         | <b>errdisable recovery</b>                 | Configures the recovery mechanis      |
|                         | <b>show errdisable detect</b>              | Displays error-disabled detection s   |
|                         | <b>show errdisable recovery</b>            | Displays error-disabled recovery ti   |
|                         | <b>show interfaces status err-disabled</b> | Displays interface status of a list o |



# clear mac address-table

To delete from the MAC address table a specific dynamic address, all dynamic addresses on a particular interface, all dynamic addresses on stack members, or all dynamic addresses on a particular VLAN, use the **clear mac address-table** command in privileged EXEC mode. This command also clears the MAC address notification global counters.

**clear mac address-table** { **dynamic** [**address** *mac-addr* | **interface** *interface-id* | **vlan** *vlan-id*] | **move update** | **notification** }

|                    |                                      |   |
|--------------------|--------------------------------------|---|
| Syntax Description | <b>dynamic</b>                       | Deletes all dynamic MAC addresses.  |
|                    | <b>address</b> <i>mac-addr</i>       | (Optional) Deletes the specified dynamic MAC address.                         |
|                    | <b>interface</b> <i>interface-id</i> | (Optional) Deletes all dynamic MAC addresses on the specified interface.      |
|                    | <b>vlan</b> <i>vlan-id</i>           | (Optional) Deletes all dynamic MAC addresses for the specified VLAN.          |
|                    | <b>move update</b>                   | Clears the MAC address table move-update counters.                            |
|                    | <b>notification</b>                  | Clears the notifications in the history table and resets the global counters. |

|                 |                                |
|-----------------|--------------------------------|
| Command Default | No default behavior or values. |
|-----------------|--------------------------------|

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

|                 |                             |                              |
|-----------------|-----------------------------|------------------------------|
| Command History | <b>Release</b>              | <b>Modification</b>          |
|                 | Cisco IOS XE Everest 16.6.1 | This command was introduced. |

|                  |  |
|------------------|--|
| Usage Guidelines | You can verify that the information was deleted by entering the <b>show mac address-table</b> command. |
|------------------|--|

This example shows how to remove a specific MAC address from the dynamic address table:

```
Device> enable
Device# clear mac address-table dynamic address 0008.0070.0007
```

|                  |   |   |
|------------------|---|---|
| Related Commands | <b>Command</b>  | <b>Description</b>  |
|                  | <b>mac address-table notification</b>                                     | Enables the MAC address notification feature.                         |
|                  | <b>mac address-table move update</b> { <b>receive</b>   <b>transmit</b> } | Configures MAC address-table move update on the device.               |
|                  | <b>show mac address-table</b>   | Displays the MAC address table static and dynamic entries.            |
|                  | <b>show mac address-table move update</b>                                 | Displays the MAC address-table move update information on the device. |

| Command                                    | Description  |
|--|--|
| <b>show mac address-table notification</b> | Displays the MAC address notification settings for all interfaces or on the specified interface when the <b>interface</b> keyword is appended. |
| <b>snmp trap mac-notification change</b>   | Enables the SNMP MAC address notification trap on a specific interface.  |

# confidentiality-offset

To enable MACsec Key Agreement protocol (MKA) to set the confidentiality offset for MACsec operations, use the **confidentiality-offset** command in MKA-policy configuration mode. To disable confidentiality offset, use the **no** form of this command.

**confidentiality-offset**  
**no confidentiality-offset**

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

**Command Default** Confidentiality offset is disabled.

**Command Modes** MKA-policy configuration (config-mka-policy)

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

## Examples

The following example shows how to enable the confidentiality offset:

```
Device> enable
Device# configure terminal
Device(config)# mka policy 2
Device(config-mka-policy)# confidentiality-offset
```

| Related Commands | Command                          | Description  |
|------------------|----------------------------------|--|
|                  | <b>mka policy</b>                | Configures an MKA policy.                                      |
|                  | <b>delay-protection</b>          | Configures MKA to use delay protection in sending MKPDU.       |
|                  | <b>include-icv-indicator</b>     | Includes ICV indicator in MKPDU.                               |
|                  | <b>key-server</b>                | Configures MKA key-server options.                             |
|                  | <b>macsec-cipher-suite</b>       | Configures cipher suite for deriving SAK.                      |
|                  | <b>sak-rekey</b>                 | Configures the SAK rekey interval.                             |
|                  | <b>send-secure-announcements</b> | Configures MKA to send secure announcements in sending MKPDUs. |
|                  | <b>ssci-based-on-sci</b>         | Computes SSCI based on the SCI.                                |
|                  | <b>use-updated-eth-header</b>    | Uses the updated Ethernet header for ICV calculation.          |

# delay-protection

To configure MKA to use delay protection in sending MACsec Key Agreement Protocol Data Units (MKPDUs), use the **delay-protection** command in MKA-policy configuration mode. To disable delay protection, use the **no** form of this command.

**delay-protection**  
**no delay-protection**

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

**Command Default** Delay protection for sending MKPDUs is disabled.

**Command Modes** MKA-policy configuration (config-mka-policy)

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

## Examples

The following example shows how to configure MKA to use delay protection in sending MKPDUs:

```
Device> enable
Device# configure terminal
Device(config)# mka policy 2
Device(config-mka-policy)# delay-protection
```

## Related Commands

| Command                          | Description  |
|----------------------------------|--|
| <b>mka policy</b>                | Configures an MKA policy.                                      |
| <b>confidentiality-offset</b>    | Sets the confidentiality offset for MACsec operations.         |
| <b>include-icv-indicator</b>     | Includes ICV indicator in MKPDU.                               |
| <b>key-server</b>                | Configures MKA key-server options.                             |
| <b>macsec-cipher-suite</b>       | Configures cipher suite for deriving SAK.                      |
| <b>sak-rekey</b>                 | Configures the SAK rekey interval.                             |
| <b>send-secure-announcements</b> | Configures MKA to send secure announcements in sending MKPDUs. |
| <b>ssci-based-on-sci</b>         | Computes SSCI based on the SCI.                                |
| <b>use-updated-eth-header</b>    | Uses the updated Ethernet header for ICV calculation.          |

## deny (MAC access-list configuration)

To prevent non-IP traffic from being forwarded if the conditions are matched, use the **deny** command in MAC access-list extended configuration mode. To remove a deny condition from the named MAC access list, use the **no** form of this command.

```
deny {any | host src-MAC-addr | src-MAC-addr mask} {any | host dst-MAC-addr |
dst-MAC-addr mask} [type mask | aarp | amber | appletalk | dec-spanning | decnet-iv |
diagnostic | dsm | etype-6000 | etype-8042 | lat | lavc-sca | lsap lsap mask | mop-console
| mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-idp] [cos cos]
no deny {any | host src-MAC-addr | src-MAC-addr mask} {any | host dst-MAC-addr |
dst-MAC-addr mask} [type mask | aarp | amber | appletalk | dec-spanning | decnet-iv |
diagnostic | dsm | etype-6000 | etype-8042 | lat | lavc-sca | lsap lsap mask | mop-console
| mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-idp] [cos cos]
```

### Syntax Description

|  |  |
|--|--|
| <b>any</b>   | Denies any source or destination MAC address.  |
| <b>host</b> <i>src-MAC-addr</i>   <i>src-MAC-addr mask</i> | Defines a host MAC address and optional subnet mask. If a packet matches the defined address, non-IP traffic from the host is denied.  |
| <b>host</b> <i>dst-MAC-addr</i>   <i>dst-MAC-addr mask</i> | Defines a destination MAC address and optional subnet mask. If a packet matches the defined address, non-IP traffic to the host is denied.   |
| <i>type mask</i>   | (Optional) Specifies the EtherType number of a packet to identify the protocol of the packet.<br><br>The type is 0 to 65535, specified in hexadecimal.<br><br>The mask is a mask of don't care bits applied to the type. |
| <b>aarp</b>  | (Optional) Specifies EtherType AppleTalk Address Resolution Protocol (ARP) address to a network address.   |
| <b>amber</b>   | (Optional) Specifies EtherType DEC-Amber.  |
| <b>appletalk</b>   | (Optional) Specifies EtherType AppleTalk/Ethernet II.  |
| <b>dec-spanning</b>  | (Optional) Specifies EtherType Digital Equipment Corporation (DEC) spanning.   |
| <b>decnet-iv</b>   | (Optional) Specifies EtherType DECnet Phase IV.  |
| <b>diagnostic</b>  | (Optional) Specifies EtherType DEC-Diagnostic.   |
| <b>dsm</b>   | (Optional) Specifies EtherType DEC-DSM.  |
| <b>etype-6000</b>  | (Optional) Specifies EtherType 0x6000.   |
| <b>etype-8042</b>  | (Optional) Specifies EtherType 0x8042.   |
| <b>lat</b>   | (Optional) Specifies EtherType DEC-LAT.  |
| <b>lavc-sca</b>  | (Optional) Specifies EtherType DEC-LAVC-SCA.   |

|                                     |   |
|-------------------------------------|---|
| <b>lsap</b> <i>lsap-number mask</i> | (Optional) Specifies the LSAP number (0 to 65535) to identify the protocol of the packet.<br><br><i>mask</i> is a mask of don't care bits applied to the LSAP number. |
| <b>mop-console</b>                  | (Optional) Specifies EtherType DEC-MOP Remote Console.  |
| <b>mop-dump</b>                     | (Optional) Specifies EtherType DEC-MOP Dump.  |
| <b>msdos</b>                        | (Optional) Specifies EtherType DEC-MSDOS.   |
| <b>mumps</b>                        | (Optional) Specifies EtherType DEC-MUMPS.   |
| <b>netbios</b>                      | (Optional) Specifies EtherType DEC- Network BIOS.   |
| <b>vines-echo</b>                   | (Optional) Specifies EtherType Virtual Integrated Banyan Systems.   |
| <b>vines-ip</b>                     | (Optional) Specifies EtherType VINES IP.  |
| <b>xns-idp</b>                      | (Optional) Specifies EtherType Xerox Network System. You can specify an arbitrary EtherType in decimal, hexadecimal, or hexadecim.                                    |
| <b>cos</b> <i>cos</i>               | (Optional) Specifies a class of service (CoS) number. CoS can be performed only in hardware. A warning message is configured.   |

**Command Default**

This command has no defaults. However, the default action for a MAC-named ACL is to deny.

**Command Modes**

MAC-access list extended configuration (config-ext-macl)

**Command History**

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

**Usage Guidelines**

You enter MAC-access list extended configuration mode by using the **mac access-list extended** global configuration command.

If you use the **host** keyword, you cannot enter an address mask; if you do not use the **host** keyword, you must enter an address mask.

When an access control entry (ACE) is added to an access control list, an implied **deny-any-any** condition exists at the end of the list. That is, if there are no matches, the packets are denied. However, before the first ACE is added, the list permits all packets.

To filter IPX traffic, you use the *type mask* or **lsap lsap mask** keywords, depending on the type of IPX encapsulation being used. Filter criteria for IPX encapsulation types as specified in Novell terminology and Cisco IOS XE terminology are listed in the table.

Table 2: IPX Filtering Criteria

| IPX Encapsulation Type |                | Filter Criterion |
|------------------------|----------------|------------------|
| Cisco IOS XE Name      | Novel Name     |                  |
| arpa                   | Ethernet II    | EtherType 0x8137 |
| snap                   | Ethernet-snap  | EtherType 0x8137 |
| sap                    | Ethernet 802.2 | LSAP 0xE0E0      |
| novell-ether           | Ethernet 802.3 | LSAP 0xFFFF      |

This example shows how to define the named MAC extended access list to deny NETBIOS traffic from any source to MAC address 00c0.00a0.03fa. Traffic matching this list is denied.

```
Device> enable
Device# configure terminal
Device(config)# mac access-list extended mac_layer
Device(config-ext-macl)# deny any host 00c0.00a0.03fa netbios.
Device(config-ext-macl)# end
```

This example shows how to remove the deny condition from the named MAC extended access list:

```
Device> enable
Device# configure terminal
Device(config)# mac access-list extended mac_layer
Device(config-ext-macl)# no deny any 00c0.00a0.03fa 0000.0000.0000 netbios.
Device(config-ext-macl)# end
```

The following example shows how to deny all packets with EtherType 0x4321:

```
Device> enable
Device# configure terminal
Device(config)# mac access-list extended mac_layer
Device(config-ext-macl)# deny any any 0x4321 0
Device(config-ext-macl)# end
```

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

#### Related Commands

| Command                         | Description  |
|---------------------------------|--|
| <b>mac access-list extended</b> | Creates an access list based on MAC addresses  |
| <b>permit</b>                   | Permits from the MAC access-list configuration<br>Permits non-IP traffic to be forwarded if condition is met |
| <b>show access-lists</b>        | Displays access control lists configured on a device   |

# 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. To remove the specification, use the **no** form of this command.

```
device-role {node | switch}
no 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 device.

## Command Default

The device role is node.

## Command Modes

IPv6 snooping configuration (config-ipv6-snooping)

## Command History

| Release                     | Modification                 |
|-----------------------------|------------------------------|
| Cisco IOS XE Everest 16.6.1 | 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> enable
Device# configure terminal
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# device-role node
Device(config-ipv6-snooping)# end
```



## 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** | **switch**}

|                           |   |   |
|---------------------------|---|---|
| <b>Syntax Description</b> | <b>host</b>   | Sets the role of the attached device to host.   |
|                           | <b>switch</b>   | Sets the role of the attached device to switch. |
| <b>Command Default</b>    | The device role is host.  |   |
| <b>Command Modes</b>      | ND inspection policy configuration (config-nd-inspection)   |   |
| <b>Command History</b>    | <b>Release</b>  | <b>Modification</b>                             |
|                           | Cisco IOS XE Everest 16.6.1   | This command was introduced.                    |
| <b>Usage Guidelines</b>   | The <b>device-role</b> 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.  |   |
|                           | The <b>switch</b> 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> enable
Device# configure terminal
Device(config)# ipv6 nd inspection policy policy1
Device(config-nd-inspection)# device-role host
Device(config-nd-inspection)# end
```

# 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*

|                           |   |                              |
|---------------------------|---|------------------------------|
| <b>Syntax Description</b> | <i>policy-name</i> 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).   |                              |
| <b>Command Default</b>    | A device tracking policy is not configured.   |                              |
| <b>Command Modes</b>      | Global configuration (config)   |                              |
| <b>Command History</b>    | <b>Release</b>  | <b>Modification</b>          |
|                           | Cisco IOS XE Everest 16.6.1   | This command was introduced. |
| <b>Usage Guidelines</b>   | <p>Use the SISF-based <b>device-tracking policy</b> command to create a device tracking policy. When the <b>device-tracking policy</b> 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:</p> <ul style="list-style-type: none"> <li>• (Optional) <b>device-role</b> {<b>node</b>}   <b>switch</b>—Specifies the role of the device attached to the port. Default is <b>node</b>.</li> <li>• (Optional) <b>limit address-count</b> <i>value</i>—Limits the number of addresses allowed per target.</li> <li>• (Optional) <b>no</b>—Negates a command or sets it to defaults.</li> <li>• (Optional) <b>destination-glean</b> {<b>recovery</b>  <b>log-only</b>} [<b>dhcp</b>]<br/>—Enables binding table recovery by data traffic source address gleaning.</li> <li>• (Optional) <b>data-glean</b> {<b>recovery</b>  <b>log-only</b>} [<b>dhcp</b>   <b>ndp</b>]<br/>—Enables binding table recovery using source or data address gleaning.</li> <li>• (Optional) <b>security-level</b> {<b>glean</b> <b>guard</b> <b>inspect</b>}—Specifies the level of security enforced by the feature. Default is <b>guard</b>. <ul style="list-style-type: none"> <li><b>glean</b>—Gleans addresses from messages and populates the binding table without any verification.</li> <li><b>guard</b>—Gleans addresses and inspects messages. In addition, it rejects RA and DHCP server messages. This is the default option.</li> <li><b>inspect</b>—Gleans addresses, validates messages for consistency and conformance, and enforces address ownership.</li> </ul> </li> <li>• (Optional) <b>tracking</b> {<b>disable</b>   <b>enable</b>}—Specifies a tracking option.</li> <li>• (Optional) <b>trusted-port</b>—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.</li> </ul> |                              |

This example shows how to configure an a device-tracking policy:

```
Device> enable
Device# configure terminal
Device(config)# device-tracking policy policy1
Device(config-device-tracking)# trusted-port
Device(config-device-tracking)# end
```

## dot1x critical (global configuration)

To configure the IEEE 802.1X critical authentication parameters, use the **dot1x critical** command in global configuration mode.

### dot1x critical eapol

|                    |  |                              |
|--------------------|--|------------------------------|
| Syntax Description | <b>eapol</b> Specifies that the switch send an EAPOL-Success message when the device successfully authenticates the critical port. |                              |
| Command Default    | <b>eapol</b> is disabled   |                              |
| Command Modes      | Global configuration (config)  |                              |
| Command History    | Release  | Modification                 |
|                    | Cisco IOS XE Everest 16.6.1  | This command was introduced. |

This example shows how to specify that the device sends an EAPOL-Success message when the device successfully authenticates the critical port:

```
Device> enable
Device# configure terminal
Device(config)# dot1x critical eapol
Device(config)# exit
```

## dot1x logging verbose

To filter detailed information from 802.1x system messages, use the **dot1x logging verbose** command in global configuration mode on a device stack or on a standalone device.

**dot1x logging verbose**  
**no dot1x logging verbose**

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> | This command has no arguments or keywords. |
|---------------------------|--|

|                        |   |
|------------------------|---|
| <b>Command Default</b> | Detailed logging of system messages is not enabled. |
|------------------------|---|

|                      |                               |
|----------------------|-------------------------------|
| <b>Command Modes</b> | Global configuration (config) |
|----------------------|-------------------------------|

|                        |                             |                              |
|------------------------|-----------------------------|------------------------------|
| <b>Command History</b> | <b>Release</b>              | <b>Modification</b>          |
|                        | Cisco IOS XE Everest 16.6.1 | This command was introduced. |

|                         |  |
|-------------------------|--|
| <b>Usage Guidelines</b> | This command filters details, such as anticipated success, from 802.1x system messages. Failure messages are not filtered. |
|-------------------------|--|

The following example shows how to filter verbose 802.1x system messages:

```
Device> enable
Device# configure terminal
Device(config)# dot1x logging verbose
Device(config)# exit
```

| Related Commands | Command                        | Description                         |
|------------------|--------------------------------|-------------------------------------|
|                  | authentication logging verbose | Filters details from authentication |
|                  | dot1x logging verbose          | Filters details from 802.1x system  |
|                  | mab logging verbose            | Filters details from MAC authentic  |

# dot1x pae

To set the Port Access Entity (PAE) type, use the **dot1x pae** command in interface configuration mode. To disable the PAE type that was set, use the **no** form of this command.

**dot1x pae** {**supplicant** | **authenticator**}  
**no dot1x pae** {**supplicant** | **authenticator**}

## Syntax Description

|                      |   |
|----------------------|---|
| <b>supplicant</b>    | The interface acts only as a supplicant and will not respond to messages that are meant for an authenticator. |
| <b>authenticator</b> | The interface acts only as an authenticator and will not respond to any messages meant for a supplicant.      |

## Command Default

PAE type is not set.

## Command Modes

Interface configuration (config-if)

## Command History

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

## Usage Guidelines

Use the **no dot1x pae** interface configuration command to disable IEEE 802.1x authentication on the port.

When you configure IEEE 802.1x authentication on a port, such as by entering the **dot1x port-control** interface configuration command, the device automatically configures the port as an IEEE 802.1x authenticator. After the **no dot1x pae** interface configuration command is entered, the Authenticator PAE operation is disabled.

The following example shows that the interface has been set to act as a supplicant:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/0/3
Device(config-if)# dot1x pae supplicant
Device(config-if)# end
```

## dot1x supplicant controlled transient

To control access to an 802.1x supplicant port during authentication, use the **dot1x supplicant controlled transient** command in global configuration mode. To open the supplicant port during authentication, use the **no** form of this command

**dot1x supplicant controlled transient**  
**no dot1x supplicant controlled transient**

### Syntax Description

This command has no arguments or keywords.

### Command Default

Access is allowed to 802.1x supplicant ports during authentication.

### Command Modes

Global configuration (config)

### Command History

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

### Usage Guidelines

In the default state, when you connect a supplicant device to an authenticator switch that has BPCU guard enabled, the authenticator port could be error-disabled if it receives a Spanning Tree Protocol (STP) bridge protocol data unit (BPDU) packets before the supplicant switch has authenticated. You can control traffic exiting the supplicant port during the authentication period. Entering the **dot1x supplicant controlled transient** command temporarily blocks the supplicant port during authentication to ensure that the authenticator port does not shut down before authentication completes. If authentication fails, the supplicant port opens. Entering the **no dot1x supplicant controlled transient** command opens the supplicant port during the authentication period. This is the default behavior.

We recommend using the **dot1x supplicant controlled transient** command on a supplicant device when BPDU guard is enabled on the authenticator switch port with the **spanning-tree bpduguard enable** interface configuration command.

This example shows how to control access to 802.1x supplicant ports on a device during authentication:

```
Device> enable
Device# configure terminal
Device(config)# dot1x supplicant controlled transient
Device(config)# exit
```

# dot1x supplicant force-multicast

To force a supplicant switch to send only multicast Extensible Authentication Protocol over LAN (EAPOL) packets whenever it receives multicast or unicast EAPOL packets, use the **dot1x supplicant force-multicast** command in global configuration mode. To return to the default setting, use the **no** form of this command.

**dot1x supplicant force-multicast**  
**no dot1x supplicant force-multicast**

## Syntax Description

This command has no arguments or keywords.

## Command Default

The supplicant device sends unicast EAPOL packets when it receives unicast EAPOL packets. Similarly, it sends multicast EAPOL packets when it receives multicast EAPOL packets.

## Command Modes

Global configuration (config)

## Command History

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

## Usage Guidelines

Enable this command on the supplicant device for Network Edge Access Topology (NEAT) to work in all host modes.

This example shows how force a supplicant device to send multicast EAPOL packets to the authenticator device:

```
Device> enable
Device# configure terminal
Device(config)# dot1x supplicant force-multicast
Device(config)# end
```

## Related Commands

| Command                     | Description                              |
|-----------------------------|--|
| <b>cisp enable</b>          | Enables CISP on a device so that it act  |
| <b>dot1x credentials</b>    | Configures the 802.1x supplicant cred    |
| <b>dot1x pae supplicant</b> | Configures an interface to act only as a |



## dot1x test eapol-capable

To monitor IEEE 802.1x activity on all the switch ports and to display information about the devices that are connected to the ports that support IEEE 802.1x, use the **dot1x test eapol-capable** command in privileged EXEC mode.

**dot1x test eapol-capable** [**interface** *interface-id*]

|                           |   |                              |
|---------------------------|---|------------------------------|
| <b>Syntax Description</b> | <b>interface</b> <i>interface-id</i> (Optional) Port to be queried. |                              |
| <b>Command Default</b>    | There is no default setting.  |                              |
| <b>Command Modes</b>      | Privileged EXEC (#)   |                              |
| <b>Command History</b>    | <b>Release</b>  | <b>Modification</b>          |
|                           | Cisco IOS XE Everest 16.6.1   | This command was introduced. |

**Usage Guidelines** Use this command to test the IEEE 802.1x capability of the devices connected to all ports or to specific ports on a switch.

There is not a no form of this command.

This example shows how to enable the IEEE 802.1x readiness check on a switch to query a port. It also shows the response received from the queried port verifying that the device connected to it is IEEE 802.1x-capable:

```
Device> enable
```

```
Device# dot1x test eapol-capable interface gigabitethernet1/0/13
```

```
DOT1X_PORT_EAPOL_CAPABLE:DOT1X: MAC 00-01-02-4b-f1-a3 on gigabitethernet1/0/13 is EAPOL capable
```

|                         |  |   |
|-------------------------|--|---|
| <b>Related Commands</b> | <b>Command</b>                           | <b>Description</b>                              |
|                         | <b>dot1x test timeout</b> <i>timeout</i> | Configures the timeout used to readiness query. |

# dot1x test timeout

To configure the timeout used to wait for EAPOL response from a port being queried for IEEE 802.1x readiness, use the **dot1x test timeout** command in global configuration mode.

**dot1x test timeout** *timeout*

|                           |                |  |
|---------------------------|----------------|--|
| <b>Syntax Description</b> | <i>timeout</i> | Time in seconds to wait for an EAPOL response. The range is from 1 to 65535 seconds. |
|---------------------------|----------------|--|

**Command Default** The default setting is 10 seconds.

**Command Modes** Global configuration (config)

| <b>Command History</b> | <b>Release</b>              | <b>Modification</b>          |
|------------------------|-----------------------------|------------------------------|
|                        | Cisco IOS XE Everest 16.6.1 | This command was introduced. |

**Usage Guidelines** Use this command to configure the timeout used to wait for EAPOL response.

There is not a no form of this command.

This example shows how to configure the switch to wait 27 seconds for an EAPOL response:

```
Device> enable
Device# dot1x test timeout 27
```

You can verify the timeout configuration status by entering the **show running-config** command.

| <b>Related Commands</b> | <b>Command</b>   | <b>Description</b>  |
|-------------------------|--|---|
|                         | <b>dot1x test eapol-capable</b> [interface <i>interface-id</i> ] | Checks for IEEE 802.1x readiness on devices connected to all or to specified IEEE 802.1x-capable ports. |

# dot1x timeout

To configure the value for retry timeouts, use the **dot1x timeout** command in global configuration or interface configuration mode. To return to the default value for retry timeouts, use the **no** form of this command.

**dot1x timeout** { **auth-period** *seconds* | **held-period** *seconds* | **quiet-period** *seconds* | **ratelimit-period** *seconds* | **server-timeout** *seconds* | **start-period** *seconds* | **supp-timeout** *seconds* | **tx-period** *seconds* }

| Syntax Description                     |  |   |
|--|--|---|
| <b>auth-period</b> <i>seconds</i>      |  | Configures the time, in seconds for which a supplicant will stay in the HELD state (that is, the length of time it will wait before trying to send the credentials again after a failed attempt).<br><br>The range is from 1 to 65535. The default is 30.   |
| <b>held-period</b> <i>seconds</i>      |  | Configures the time, in seconds for which a supplicant will stay in the HELD state (that is, the length of time it will wait before trying to send the credentials again after a failed attempt).<br><br>The range is from 1 to 65535. The default is 60.   |
| <b>quiet-period</b> <i>seconds</i>     |  | Configures the time, in seconds, that the authenticator (server) remains quiet (in the HELD state) following a failed authentication exchange before trying to reauthenticate the client.<br><br>The range is from 1 to 65535. The default is 60.   |
| <b>ratelimit-period</b> <i>seconds</i> |  | Throttles the EAP-START packets that are sent from misbehaving client PCs (for example, PCs that send EAP-START packets that result in the wasting of device processing power). <ul style="list-style-type: none"> <li>• The authenticator ignores EAPOL-Start packets from clients that have successfully authenticated for the rate-limit period duration.</li> <li>• The range is from 1 to 65535. By default, rate limiting is disabled.</li> </ul> |
| <b>server-timeout</b> <i>seconds</i>   |  | Configures the interval, in seconds, between two successive EAPOL-Start frames when they are being retransmitted. <ul style="list-style-type: none"> <li>• The range is from 1 to 65535. The default is 30.</li> </ul> <p>If the server does not send a response to an 802.1X packet within the specified period, the packet is sent again.</p>   |
| <b>start-period</b> <i>seconds</i>     |  | Configures the interval, in seconds, between two successive EAPOL-Start frames when they are being retransmitted.<br><br>The range is from 1 to 65535. The default is 30.   |

|                                    |  |
|------------------------------------|--|
| <b>supp-timeout</b> <i>seconds</i> | Sets the authenticator-to-suppliant retransmission time for all EAP messages other than EAP Request ID.<br><br>The range is from 1 to 65535. The default is 30.  |
| <b>tx-period</b> <i>seconds</i>    | Configures the number of seconds between retransmission of EAP request ID packets (assuming that no response is received) to the client.<br><br><ul style="list-style-type: none"> <li>• The range is from 1 to 65535. The default is 30.</li> <li>• If an 802.1X packet is sent to the supplicant and the supplicant does not send a response after the retry period, the packet will be sent again.</li> </ul> |

|                        |  |
|------------------------|--|
| <b>Command Default</b> | Periodic reauthentication and periodic rate-limiting are done. |
|------------------------|--|

|                      |  |
|----------------------|--|
| <b>Command Modes</b> | Global configuration (config)<br><br>Interface configuration (config-if) |
|----------------------|--|

|                        |                             |                              |
|------------------------|-----------------------------|------------------------------|
| <b>Command History</b> | <b>Release</b>              | <b>Modification</b>          |
|                        | Cisco IOS XE Everest 16.6.1 | This command was introduced. |

**Usage Guidelines**

You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers.

The **dot1x timeout reauth-period** interface configuration command affects the behavior of the device only if you have enabled periodic re-authentication by using the **dot1x reauthentication** interface configuration command.

During the quiet period, the device does not accept or initiate any authentication requests. If you want to provide a faster response time to the user, enter a number smaller than the default.

When the **ratelimit-period** is set to 0 (the default), the device does not ignore EAPOL packets from clients that have been successfully authenticated and forwards them to the RADIUS server.

The following example shows that various 802.1X retransmission and timeout periods have been set:

```
Device> enable
Device(config)# configure terminal
Device(config)# interface gigabitethernet 1/0/3
Device(config-if)# dot1x port-control auto
Device(config-if)# dot1x timeout auth-period 2000
Device(config-if)# dot1x timeout held-period 2400
Device(config-if)# dot1x timeout quiet-period 600
Device(config-if)# dot1x timeout start-period 90
Device(config-if)# dot1x timeout supp-timeout 300
Device(config-if)# dot1x timeout tx-period 60
Device(config-if)# dot1x timeout server-timeout 60
Device(config-if)# end
```

# dtls

To configure Datagram Transport Layer Security (DTLS) parameters, use the **dtls** command in radius server configuration mode. To return to the default setting, use the **no** form of this command.

**dtls** [**connectiontimeout** *connection-timeout-value*] [**idletimeout** *idle-timeout-value*] [**ip** {**radius source-interface** *interface-name* | **vrf forwarding** *forwarding-table-name*}] [**port** *port-number*] [**retries** *number-of-connection-retries*] [**trustpoint** {**client** *trustpoint name* | **server** *trustpoint name*}]

**no dtls**

## Syntax Description

|   |  |
|---|--|
| <b>connectiontimeout</b> <i>connection-timeout-value</i>  | (Optional) Configures the DTLS connection timeout value.                 |
| <b>idletimeout</b> <i>idle-timeout-value</i>  | (Optional) Configures the DTLS idle timeout value.                       |
| <b>ip</b> { <b>radius source-interface</b> <i>interface-name</i>   <b>vrf forwarding</b> <i>forwarding-table-name</i> } | (Optional) Configures IP source parameters.                              |
| <b>port</b> <i>port-number</i>  | (Optional) Configures the DTLS port number.                              |
| <b>retries</b> <i>number-of-connection-retries</i>  | (Optional) Configures the number of DTLS connection retries.             |
| <b>trustpoint</b> { <b>client</b> <i>trustpoint name</i>   <b>server</b> <i>trustpoint name</i> }                       | (Optional) Configures the DTLS trustpoint for the client and the server. |

## Command Default

- The default value of DTLS connection timeout is 5 seconds.
- The default value of DTLS idle timeout is 60 seconds.
- The default DTLS port number is 2083.
- The default value of DTLS connection retries is 5.

## Command Modes

Radius server configuration (config-radius-server)

## Command History

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

## Usage Guidelines

We recommend that you use the same server type, either only Transport Layer Security (TLS) or only DTLS, under an Authentication, Authorization, and Accounting (AAA) server group.

## Examples

The following example shows how to configure the DTLS connection timeout value to 10 seconds:

```
Device> enable
Device# configure terminal
Device(config)# radius server R1
```

```
Device(config-radius-server)# dtls connectiontimeout 10
Device(config-radius-server)# end
```

**Related Commands**

| Command   | Description                                      |
|---|--|
| <b>show aaa servers</b>   | Displays information related to the DTLS server. |
| <b>clear aaa counters servers radius</b> <i>{server id   all}</i> | Clears the RADIUS DTLS-specific statistics.      |
| <b>debug radius dtls</b>  | Enables RADIUS DTLS-specific debugs.             |

# enable password

To set a local password to control access to various privilege levels, use the **enable password** command in global configuration mode. To remove control access of the local password, use the **no** form of this command.

**enable password** [**level** *level*] {[**0**] *unencrypted-password* | [*encryption-type*] *encrypted-password*}  
**no enable password** [**level** *level*]

| Syntax Description | <b>level</b> <i>level</i>   | (Optional) Specifies the level for which the password is applicable. You can specify levels, using numbers 0 through 15. Level 1 is normal user EXEC mode user privilege level. If not specified in the command or in the <b>no</b> form of the command, the privilege level is 1.            |
|--------------------|-----------------------------|---|
|                    | <b>0</b>                    | (Optional) Specifies an unencrypted cleartext password. The password is converted to a SHA-256 secret and is stored in the device.  |
|                    | <i>unencrypted-password</i> | Specifies the password to enter enable mode.  |
|                    | <i>encryption-type</i>      | (Optional) Cisco-proprietary algorithm used to encrypt the password. If you specify an encryption type, the next argument that you supply must be an encrypted password (a password already encrypted on the device). You can specify type 7, which indicates that a hidden password follows. |
|                    | <i>encrypted-password</i>   | Encrypted password copied from another device configuration.  |

**Command Default** No password is defined.

**Command Modes** Global configuration (config)

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

**Usage Guidelines** If neither the **enable password** command nor the **enable secret** command is configured, and if a line password is configured for the console, the console line password serves as the enable password for all VTY (Telnet and Secure Shell [SSH]) sessions.

Use **enable password** command with the **level** option to define a password for a specific privilege level. After you specify the level and the password, share the password with users who need to access this level. Use the **privilege level** configuration command to specify the commands that are accessible at various levels.

Typically, you enter an encryption type only if you copy and paste a password that has already been encrypted by a Cisco device, into this command.



**Caution** If you specify an encryption type and then enter a cleartext password, you will not be able to re-enter enable mode. You cannot recover a lost password that has been encrypted earlier.

If the **service password-encryption** command is set, the encrypted form of the password you create with the **enable password** command is displayed when the **more nvram:startup-config** command is run.

You can enable or disable password encryption with the **service password-encryption** command.

An enable password is defined as follows:

- Must contain a combination of numerals from 1 to 25, and uppercase and lowercase alphanumeric characters.
- Can have leading spaces, but they are ignored. However, intermediate and trailing spaces are recognized.
- Can contain the question mark (?) character if you precede the question mark with the key combination Crtl-V when you create the password, for example, to create the password *abc?123*, do the following:
  1. Enter **abc**.
  2. Press **Crtl-v**.
  3. Enter **?123**.



**Note** When the system prompt you to enter the **enable password** command, you need not precede the question mark with Ctrl-V; you can enter *abc?123* at the password prompt.

## Examples

The following example shows how to enable the password *pswd2* for privilege level 2:

```
Device> enable
Device# configure terminal
Device(config)# enable password level 2 pswd2
```

The following example shows how to set the encrypted password *\$1\$i5Rkls3LoyxzS8t9*, which has been copied from a device configuration file, for privilege level 2 using encryption type 7:

```
Device> enable
Device# configure terminal
Device(config)# enable password level 2 5 $1$i5Rkls3LoyxzS8t9
```

## Related Commands

| Command                            | Description   |
|------------------------------------|---|
| <b>enable secret</b>               | Specifies an additional layer of security over the <b>enable password</b> .                   |
| <b>service password-encryption</b> | Encrypts a password.  |
| <b>more nvram:startup-config</b>   | Displays the startup configuration file contained in NVRAM. CONFIG_FILE environment variable. |
| <b>privilege level</b>             | Sets the privilege level for the user.  |



# enable secret

To specify an additional layer of security over the **enable password** command, use the **enable secret** command in global configuration mode. To turn off the enable secret function, use the **no** form of this command.

**enable secret** [**level** *level*] {[**0**] *unencrypted-password* | *encryption-type encrypted-password*}  
**no enable secret** [**level** *level*] [*encryption-type encrypted-password*]

| Syntax Description | <b>level</b> <i>level</i>   | (Optional) Specifies the level for which the password is applicable. You can specify levels, using numerals 1 through 15. Level 1 is normal user EXEC mode privileges in the command or in the <b>no</b> form of the command, the privilege level defaults to 15.   |
|--------------------|---|---|
|                    | <b>0</b>  | (Optional) Specifies an unencrypted cleartext password. The password is converted to a SHA-256 secret and is stored in the device.  |
|                    | <i>unencrypted-password</i>   | Specifies the password for users to enter enable mode. This password should be different from the enable password created with the <b>enable password</b> command.  |
|                    | <i>encryption-type</i>  | Cisco-proprietary algorithm used to hash the password: <ul style="list-style-type: none"> <li>• <b>5</b>: Specifies a message digest algorithm 5-encrypted (MD5-encrypted) secret.</li> <li>• <b>8</b>: Specifies a Password-Based Key Derivation Function 2 (PBKDF2) with 9600 iterations.</li> <li>• <b>9</b>: Specifies a scrypt-hashed secret.</li> </ul> |
|                    | <i>encrypted-password</i>   | Hashed password that is copied from another device configuration.   |
| Command Default    | No password is defined.   |   |
| Command Modes      | Global configuration (config)   |   |
| Command History    | Release   | Modification  |
|                    | Cisco IOS XE Everest 16.6.1   | This command was introduced.  |
| Usage Guidelines   | <p>If neither the <b>enable password</b> command or the <b>enable secret</b> command is configured, and if a line password is configured for the console, the console line password serves as the enable password for all vty (Telnet and Secure Shell [SSH]) sessions.</p> <p>Use the <b>enable secret</b> command to provide an additional layer of security over the <b>enable password</b> password. The <b>enable secret</b> command provides better security by storing the password using a nonreversible cryptographic function. The additional layer of security encryption is useful in environments where the password is sent to the network or is stored on a TFTP server.</p> <p>Typically, you enter an encryption type only when you paste an encrypted password that you copied from a device configuration file, into this command.</p> |   |

**Caution**

If you specify an encryption type and then enter a cleartext password, you will not be able to reenter enable mode. You cannot recover a lost password that has been encrypted earlier.

If you use the same password for the **enable password** and **enable secret** commands, you receive an error message warning that this practice is not recommended, but the password will be accepted. By using the same password, however, you undermine the additional security the **enable secret** command provides.

**Note**

After you set a password using the **enable secret** command, a password set using the **enable password** command works only if the **enable secret** is disabled. Additionally, you cannot recover a lost password that has been encrypted by any method.

If the **service password-encryption** command is set, the encrypted form of the password you create is displayed when the **more nvram:startup-config** command is run.

You can enable or disable password encryption with the **service password-encryption** command.

An enable password is defined as follows:

- Must contain a combination of numerals from 1 to 25, and uppercase and lowercase alphanumeric characters.
- Can have leading spaces, but they are ignored. However, intermediate and trailing spaces are recognized.
- Can contain the question mark (?) character if you precede the question mark with the key combination Ctrl-v when you create the password; for example, to create the password *abc?123*, do the following:
  1. Enter **abc**.
  2. Press **Ctrl-v**.
  3. Enter **?123**.

**Note**

When the system prompts you to enter the **enable password** command, you need not precede the question mark with Ctrl-v; you can enter **abc?123** at the password prompt.

**Examples**

The following example shows how to specify a password with the **enable secret** command:

```
Device> enable
Device# configure terminal
Device(config)# enable secret password
```

After specifying a password with the **enable secret** command, users must enter this password to gain access. Otherwise, passwords set using the **enable password** command will no longer work.

```
Password: password
```

The following example shows how to enable the encrypted password \$1\$FaD0\$Xyti5Rkls3LoyxzS8, which has been copied from a device configuration file, for privilege level 2, using the encryption type 4:

```
Device> enable
Device# configure terminal
Device(config)# enable password level 2 4 $1$FaD0$Xyti5Rkls3LoyxzS8
```

The following example shows the warning message that is displayed when a user enters the **enable secret 4 encrypted-password** command:

```
Device> enable
Device# configure terminal
Device(config)# enable secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY
```

WARNING: Command has been added to the configuration but Type 4 passwords have been deprecated.  
Migrate to a supported password type

```
Device(config)# end
Device# show running-config | inc secret
```

```
enable secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY
```

#### Related Commands

| Command                            | Description   |
|------------------------------------|---|
| <b>enable password</b>             | Sets a local password to control access to various privileges.                                    |
| <b>more nvram:startup-config</b>   | Displays the startup configuration file contained in NVRAM. The CONFIG_FILE environment variable. |
| <b>service password-encryption</b> | Encrypt passwords.  |

# epm access-control open

To configure an open directive for ports that do not have an access control list (ACL) configured, use the **epm access-control open** command in global configuration mode. To disable the open directive, use the **no** form of this command.

**epm access-control open**  
**no epm access-control open**

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

**Command Default** The default directive applies.

**Command Modes** Global configuration (config)

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

**Usage Guidelines** Use this command to configure an open directive that allows hosts without an authorization policy to access ports configured with a static ACL. If you do not configure this command, the port applies the policies of the configured ACL to the traffic. If no static ACL is configured on a port, both the default and open directives allow access to the port.

You can verify your settings by entering the **show running-config** command.

This example shows how to configure an open directive.

```
Device> enable
Device# configure terminal
Device(config)# epm access-control open
Device(config)# exit
```

| Related Commands | Command                    | Description  |
|------------------|----------------------------|--|
|                  | <b>show running-config</b> | Displays the contents of the current running configuration file. |

# include-icv-indicator

To include the integrity check value (ICV) indicator in MKPDU, use the **include-icv-indicator** command in MKA-policy configuration mode. To disable the ICV indicator, use the **no** form of this command.

**include-icv-indicator**  
**no include-icv-indicator**

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

**Command Default** ICV indicator is included.

**Command Modes** MKA-policy configuration (config-mka-policy)

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

## Examples

The following example shows how to include the ICV indicator in MKPDU:

```
Device> enable
Device# configure terminal
Device(config)# mka policy 2
Device(config-mka-policy)# include-icv-indicator
```

## Related Commands

| Command                          | Description  |
|----------------------------------|--|
| <b>mka policy</b>                | Configures an MKA policy.                                      |
| <b>confidentiality-offset</b>    | Sets the confidentiality offset for MACsec operations.         |
| <b>delay-protection</b>          | Configures MKA to use delay protection in sending MKPDU.       |
| <b>key-server</b>                | Configures MKA key-server options.                             |
| <b>macsec-cipher-suite</b>       | Configures cipher suite for deriving SAK.                      |
| <b>sak-rekey</b>                 | Configures the SAK rekey interval.                             |
| <b>send-secure-announcements</b> | Configures MKA to send secure announcements in sending MKPDUs. |
| <b>ssci-based-on-sci</b>         | Computes SSCI based on the SCI.                                |
| <b>use-updated-eth-header</b>    | Uses the updated Ethernet header for ICV calculation.          |

## ip access-list

To define an IP access list or object-group access control list (ACL) by name or number or to enable filtering for packets with IP helper-address destinations, use the **ip access-list** command in global configuration mode. To remove the IP access list or object-group ACL or to disable filtering for packets with IP helper-address destinations, use the **no** form of this command.

**ip access-list** [{**extended** | **resequence** | **standard**} {*access-list-number**access-list-name*} | **helper egress check** | **log-update threshold** *threshold-number* | **logging** {**hash-generation** | **interval** *time*} | **persistent** | **role-based** *access-list-name*}

**ip access-list** [{**extended** | **resequence** | **standard**} {*access-list-number**access-list-name*} | **helper egress check** | **log-update threshold** | **logging** {**hash-generation** | **interval**} | **persistent** | **role-based** *access-list-name*}

### Syntax Description

|   |   |
|---|---|
| <b>standard</b>                             | Specifies a standard IP access list.  |
| <b>resequence</b>                           | Specifies a resequenced IP access list.   |
| <b>extended</b>                             | Specifies an extended IP access list. Required for object-group ACLs.   |
| <i>access-list-name</i>                     | Name of the IP access list or object-group ACL. Names cannot contain a space or quotation mark, and must begin with an alphabetic character to prevent ambiguity with numbered access lists.                              |
| <i>access-list-number</i>                   | Number of the access list. <ul style="list-style-type: none"> <li>• A standard IP access list is in the ranges 1-99 or 1300-1999.</li> <li>• An extended IP access list is in the ranges 100-199 or 2000-2699.</li> </ul> |
| <b>helper egress check</b>                  | Enables permit or deny matching capability for an outbound access list that is applied to an interface, for traffic that is relayed via the IP helper feature to a destination server address.                            |
| <b>log-update</b>                           | Controls the access list log updates.   |
| <b>threshold</b><br><i>threshold-number</i> | Sets the access list logging threshold. The range is 0 to 2147483647.   |
| <b>logging</b>                              | Controls the access list logging.   |
| <b>hash-generation</b>                      | Enables syslog hash code generation.  |
| <b>interval</b> <i>time</i>                 | Sets the access list logging interval in milliseconds. The range is 0 to 2147483647.  |
| <b>persistent</b>                           | Access control entry (ACE) sequence numbers are persistent across reloads.<br><b>Note</b> This is enabled by default and cannot be disabled.  |
| <b>role-based</b>                           | Specifies a role-based IP access list.  |

**Command Default**

No IP access list or object-group ACL is defined, and outbound ACLs do not match and filter IP helper relayed traffic.

**Command Modes**

Global configuration (config)

**Command History**

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

**Usage Guidelines**

Use this command to configure a named or numbered IP access list or an object-group ACL. This command places the device in access-list configuration mode, where you must define the denied or permitted access conditions by using the **deny** and **permit** commands.

Specifying the **standard** or **extended** keyword with the **ip access-list** command determines the prompt that appears when you enter access-list configuration mode. You must use the **extended** keyword when defining object-group ACLs.

You can create object groups and IP access lists or object-group ACLs independently, which means that you can use object-group names that do not yet exist.

Use the **ip access-group** command to apply the access list to an interface.

The **ip access-list helper egress check** command enables outbound ACL matching for permit or deny capability on packets with IP helper-address destinations. When you use an outbound extended ACL with this command, you can permit or deny IP helper relayed traffic based on source or destination User Datagram Protocol (UDP) ports. The **ip access-list helper egress check** command is disabled by default; outbound ACLs will not match and filter IP helper relayed traffic.

**Examples**

The following example defines a standard access list named Internetfilter:

```
Device> enable
Device# configure terminal
Device(config)# ip access-list standard Internetfilter
Device(config-std-nacl)# permit 192.168.255.0 0.0.0.255
Device(config-std-nacl)# permit 10.88.0.0 0.0.255.255
Device(config-std-nacl)# permit 10.0.0.0 0.255.255.255
```

The following example shows how to create an object-group ACL that permits packets from the users in my\_network\_object\_group if the protocol ports match the ports specified in my\_service\_object\_group:

```
Device> enable
Device# configure terminal
Device(config)# ip access-list extended my_ogacl_policy
Device(config-ext-nacl)# permit tcp object-group my_network_object_group portgroup
my_service_object_group any
Device(config-ext-nacl)# deny tcp any any
```

The following example shows how to enable outbound ACL filtering on packets with helper-address destinations:

```
Device> enable
Device# configure terminal
Device(config)# ip access-list helper egress check
```

**Related Commands**

| <b>Command</b>              | <b>Description</b>  |
|-----------------------------|---|
| <b>deny</b>                 | Sets conditions in a named IP access list or in an object-group ACL that will deny packets.   |
| <b>ip access-group</b>      | Applies an ACL or an object-group ACL to an interface or a service policy map.                |
| <b>object-group network</b> | Defines network object groups for use in object-group ACLs.                                   |
| <b>object-group service</b> | Defines service object groups for use in object-group ACLs.                                   |
| <b>permit</b>               | Sets conditions in a named IP access list or in an object-group ACL that will permit packets. |
| <b>show ip access-list</b>  | Displays the contents of IP access lists or object-group ACLs.                                |
| <b>show object-group</b>    | Displays information about object groups that are configured.                                 |



## ip access-list role-based

To create a role-based (security group) access control list (RBACL) and enter role-based ACL configuration mode, use the **ip access-list role-based** command in global configuration mode. To remove the configuration, use the **no** form of this command.

```
ip access-list role-based access-list-name
no ip access-list role-based access-list-name
```

|                           |   |
|---------------------------|---|
| <b>Syntax Description</b> | <i>access-list-name</i> Name of the security group access control list (SGACL). |
|---------------------------|---|

|                        |                                     |
|------------------------|-------------------------------------|
| <b>Command Default</b> | Role-based ACLs are not configured. |
|------------------------|-------------------------------------|

|                      |                               |
|----------------------|-------------------------------|
| <b>Command Modes</b> | Global configuration (config) |
|----------------------|-------------------------------|

|                        |                             |                              |
|------------------------|-----------------------------|------------------------------|
| <b>Command History</b> | <b>Release</b>              | <b>Modification</b>          |
|                        | Cisco IOS XE Everest 16.6.1 | This command was introduced. |

|                         |   |
|-------------------------|---|
| <b>Usage Guidelines</b> | For SGACL logging, you must configure the <b>permit ip log</b> command. Also, this command must be configured in Cisco Identity Services Engine (ISE) to enable logging for dynamic SGACLs. |
|-------------------------|---|

The following example shows how to define an SGACL that can be applied to IPv4 traffic and enter role-based access list configuration mode:

```
Device> enable
Device# configure terminal
Device(config)# ip access-list role-based rbac11
Device(config-rb-acl)# permit ip log
Device(config-rb-acl)# end
```

| <b>Related Commands</b> | Command                    | Description  |
|-------------------------|----------------------------|--|
|                         | <b>permit ip log</b>       | Permits logging that matches the configured entry. |
|                         | <b>show ip access-list</b> | Displays contents of all current IP access lists.  |

# ip admission

To enable web authentication, use the **ip admission** command in interface configuration mode or fallback-profile configuration mode. To disable web authentication, use the **no** form of this command.

**ip admission** *rule*  
**no ip admission** *rule*

|                           |                                     |
|---------------------------|-------------------------------------|
| <b>Syntax Description</b> | <i>rule</i> IP admission rule name. |
|---------------------------|-------------------------------------|

|                        |                                 |
|------------------------|---------------------------------|
| <b>Command Default</b> | Web authentication is disabled. |
|------------------------|---------------------------------|

|                      |   |
|----------------------|---|
| <b>Command Modes</b> | Interface configuration (config-if)<br>Fallback-profile configuration (config-fallback-profile) |
|----------------------|---|

| <b>Command History</b> | <b>Release</b>              | <b>Modification</b>          |
|------------------------|-----------------------------|------------------------------|
|                        | Cisco IOS XE Everest 16.6.1 | This command was introduced. |

|                         |   |
|-------------------------|---|
| <b>Usage Guidelines</b> | The <b>ip admission</b> command applies a web authentication rule to a switch port. |
|-------------------------|---|

This example shows how to apply a web authentication rule to a switchport:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip admission rule1
Device(config-if)# end
```

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> enable
Device# configure terminal
Device(config)# fallback profile profile1
Device(config-fallback-profile)# ip admission rule1
Device(config-fallback-profile)# end
```

# ip admission name

To enable web authentication, use the **ip admission name** command in global configuration mode. To disable web authentication, use the **no** form of this command.

**ip admission name** *name* {**consent** | **proxy http**} [**absolute timer** *minutes* | **inactivity-time** *minutes* | **list** {*acl* | *acl-name*} | **service-policy type tag** *service-policy-name*]  
**no ip admission name** *name* {**consent** | **proxy http**} [**absolute timer** *minutes* | **inactivity-time** *minutes* | **list** {*acl* | *acl-name*} | **service-policy type tag** *service-policy-name*]

| Syntax Description     |                                       |   |
|------------------------|---------------------------------------|---|
|                        | <i>name</i>                           | Name of network admission control rule.   |
|                        | <b>consent</b>                        | Associates an authentication proxy consent web page with the IP admission rule specified using the <i>admission-name</i> argument.  |
|                        | <b>proxy http</b>                     | Configures web authentication custom page.  |
|                        | <b>absolute-timer</b> <i>minutes</i>  | (Optional) Elapsed time, in minutes, before the external server times out.  |
|                        | <b>inactivity-time</b> <i>minutes</i> | (Optional) Elapsed time, in minutes, before the external file server is deemed unreachable.   |
|                        | <b>list</b>                           | (Optional) Associates the named rule with an access control list (ACL).   |
|                        | <i>acl</i>                            | Applies a standard, extended list to a named admission control rule. The value ranges from 1 through 199, or from 1300 through 2699 for expanded range.   |
|                        | <i>acl-name</i>                       | Applies a named access list to a named admission control rule.  |
|                        | <b>service-policy type tag</b>        | (Optional) A control plane service policy is to be configured.  |
|                        | <i>service-policy-name</i>            | Control plane tag service policy that is configured using the <b>policy-map type control tag</b> <i>polycyname</i> command, keyword, and argument. This policy map is used to apply the actions on the host when a tag is received. |
| <b>Command Default</b> | Web authentication is disabled.       |   |
| <b>Command Modes</b>   | Global configuration (config)         |   |
| <b>Command History</b> | <b>Release</b>                        | <b>Modification</b>   |
|                        | Cisco IOS XE Everest 16.6.1           | This command was introduced.  |

## Usage Guidelines

The **ip admission name** command globally enables web authentication on a switch.

After you enable web authentication on a switch, use the **ip access-group in** and **ip admission web-rule** interface configuration commands to enable web authentication on a specific interface.

## Examples

This example shows how to configure only web authentication on a switch port:

```
Device> enable
Device# configure terminal
Device(config) ip admission name http-rule proxy http
Device(config) # interface gigabitethernet1/0/1
Device(config-if) # ip access-group 101 in
Device(config-if) # ip admission rule
Device(config-if) # end
```

This example shows how to configure IEEE 802.1x authentication with web authentication as a fallback mechanism on a switch port:

```
Device> enable
Device# configure terminal
Device(config) # ip admission name rule2 proxy http
Device(config) # fallback profile profile1
Device(config) # ip access group 101 in
Device(config) # ip admission name rule2
Device(config) # interface gigabitethernet1/0/1
Device(config-if) # dot1x port-control auto
Device(config-if) # dot1x fallback profile1
Device(config-if) # end
```

## Related Commands

| Command   | Description  |
|---|--|
| <b>dot1x fallback</b>   | Configures a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication. |
| <b>fallback profile</b>   | Creates a web authentication fallback profile.   |
| <b>ip admission</b>   | Enables web authentication on a port.  |
| <b>show authentication sessions interface <i>interface</i> detail</b> | Displays information about the web authentication session status.  |
| <b>show ip admission</b>  | Displays information about NAC cached entries or the NAC configuration.  |

# ip dhcp snooping database

To configure the Dynamic Host Configuration Protocol (DHCP)-snooping database, use the **ip dhcp snooping database** command in global configuration mode. To disable the DHCP-snooping database, use the **no** form of this command.

```
ip dhcp snooping database { crashinfo: url | flash: url | ftp: url | http: url | https: url
| rcp: url | scp: url | tftp: url | timeout seconds | usbflash0: url | write-delay
seconds }
no ip dhcp snooping database [ timeout | write-delay ]
abor
```

| Syntax Description |                               |  |
|--------------------|-------------------------------|--|
|                    | <b>crashinfo:</b> <i>url</i>  | Specifies the database URL for storing entries using crashinfo.                  |
|                    | <b>flash:</b> <i>url</i>      | Specifies the database URL for storing entries using flash.                      |
|                    | <b>ftp:</b> <i>url</i>        | Specifies the database URL for storing entries using FTP.                        |
|                    | <b>http:</b> <i>url</i>       | Specifies the database URL for storing entries using HTTP.                       |
|                    | <b>https:</b> <i>url</i>      | Specifies the database URL for storing entries using secure HTTP (https).        |
|                    | <b>rcp:</b> <i>url</i>        | Specifies the database URL for storing entries using remote copy (rcp).          |
|                    | <b>scp:</b> <i>url</i>        | Specifies the database URL for storing entries using Secure Copy (SCP).          |
|                    | <b>tftp:</b> <i>url</i>       | Specifies the database URL for storing entries using TFTP.                       |
|                    | <b>timeout</b> <i>seconds</i> | Specifies the cancel timeout interval; valid values are from 0 to 86400 seconds. |
|                    | <b>usbflash0:</b> <i>url</i>  | Specifies the database URL for storing entries using USB flash.                  |

---

**write-delay** *seconds*

---

Specifies the amount of time before writing the DHCP-snooping entries to an external server after a change is seen in the local DHCP-snooping database; valid values are from 15 to 86400 seconds.

---



---

**Command Default** The DHCP-snooping database is not configured.

---

**Command Modes** Global configuration (config)

---

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

---



---

**Usage Guidelines** You must enable DHCP snooping on the interface before entering this command. Use the **ip dhcp snooping** command to enable DHCP snooping.

This example shows how to specify the database URL using TFTP:

```
Device> enable
Device# configure terminal
Device(config)# ip dhcp snooping database tftp://10.90.90.90/snooping-rp2
Device(config)# exit
```

This example shows how to specify the amount of time before writing DHCP snooping entries to an external server:

```
Device> enable
Device# configure terminal
Device(config)# ip dhcp snooping database write-delay 15
Device(config)# exit
```

# ip dhcp snooping information option format remote-id

To configure the option-82 remote-ID suboption, use the **ip dhcp snooping information option format remote-id** command in global configuration mode on the device to configure the option-82 remote-ID suboption. To configure the default remote-ID suboption, use the **no** form of this command.

**ip dhcp snooping information option format remote-id** {hostname | string *string*}  
**no ip dhcp snooping information option format remote-id** {hostname | string *string*}

|                    |   |   |
|--------------------|---|---|
| Syntax Description | <b>hostname</b>   | Specify the device hostname as the remote ID.                         |
|                    | <b>string</b> <i>string</i>   | Specify a remote ID, using from 1 to 63 ASCII characters (no spaces). |
| Command Default    | The device MAC address is the remote ID.  |   |
| Command Modes      | Global configuration (config)   |   |
| Command History    | <b>Release</b>  | <b>Modification</b>   |
|                    | Cisco IOS XE Everest 16.6.1   | This command was introduced.  |
| Usage Guidelines   | You must globally enable DHCP snooping by using the <b>ip dhcp snooping</b> global configuration command for any DHCP snooping configuration to take effect.  |   |
|                    | When the option-82 feature is enabled, the default remote-ID suboption is the device MAC address. This command allows you to configure either the device hostname or a string of up to 63 ASCII characters (but no spaces) to be the remote ID. |   |



**Note** If the hostname exceeds 63 characters, it will be truncated to 63 characters in the remote-ID configuration.

This example shows how to configure the option- 82 remote-ID suboption:

```
Device> enable
Device# configure terminal
Device(config)# ip dhcp snooping information option format remote-id hostname
Device(config)# exit
```

# ip dhcp snooping verify no-relay-agent-address

To disable the DHCP snooping feature from verifying that the relay agent address (giaddr) in a DHCP client message matches the client hardware address on an untrusted port, use the **ip dhcp snooping verify no-relay-agent-address** command in global configuration mode. To enable verification, use the **no** form of this command.

**ip dhcp snooping verify no-relay-agent-address**  
**no ip dhcp snooping verify no-relay-agent-address**

## Syntax Description

This command has no arguments or keywords.

## Command Default

The DHCP snooping feature verifies that the relay-agent IP address (giaddr) field in DHCP client message on an untrusted port is 0.

## Command Modes

Global configuration (config)

## Command History

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

## Usage Guidelines

By default, the DHCP snooping feature verifies that the relay-agent IP address (giaddr) field in DHCP client message on an untrusted port is 0; the message is dropped if the giaddr field is not 0. Use the **ip dhcp snooping verify no-relay-agent-address** command to disable the verification. Use the **no ip dhcp snooping verify no-relay-agent-address** to reenale verification.

This example shows how to enable verification of the giaddr in a DHCP client message:

```
Device> enable
Device# configure terminal
Device(config)# no ip dhcp snooping verify no-relay-agent-address
Device(config)# exit
```



## ip http access-class

To specify the access list that should be used to restrict access to the HTTP server, use the **ip http access-class** command in global configuration mode. To remove a previously configured access list association, use the **no** form of this command.

```
ip http access-class { access-list-number | ipv4 { access-list-number | access-list-name } |
ipv6 access-list-name }
no ip http access-class { access-list-number | ipv4 { access-list-number | access-list-name }
| ipv6 access-list-name }
```

### Syntax Description

|                           |  |
|---------------------------|--|
| <i>access-list-number</i> | Standard IP access list number in the range 0 to 99, as configured by the <b>access-list</b> global configuration command. |
| <b>ipv4</b>               | Specifies the IPv4 access list to restrict access to the secure HTTP server.   |
| <i>access-list-name</i>   | Name of a standard IPv4 access list, as configured by the <b>ip access-list</b> command.                                   |
| <b>ipv6</b>               | Specifies the IPv6 access list to restrict access to the secure HTTP server.   |

### Command Default

No access list is applied to the HTTP server.

### Command Modes

Global configuration (config)

### Command History

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

### Usage Guidelines

If this command is configured, the specified access list is assigned to the HTTP server. Before the HTTP server accepts a connection, it checks the access list. If the check fails, the HTTP server does not accept the request for a connection.

### Examples

The following example shows how to define an access list as 20 and assign it to the HTTP server:

```
Device> enable
Device(config)# ip access-list standard 20
Device(config-std-nacl)# permit 209.165.202.130 0.0.0.255
Device(config-std-nacl)# permit 209.165.201.1 0.0.255.255
Device(config-std-nacl)# permit 209.165.200.225 0.255.255.255
Device(config-std-nacl)# exit
Device(config)# ip http access-class 20
Device(config-std-nacl)# exit
```

The following example shows how to define an IPv4 named access list as and assign it to the HTTP server.

```
Device> enable
Device(config)# ip access-list standard Internet_filter
Device(config-std-nacl)# permit 1.2.3.4
Device(config-std-nacl)# exit
```

```
Device(config)# ip http access-class ipv4 Internet_filter
Device(config)# exit
```

**Related Commands**

| Command               | Description  |
|-----------------------|--|
| <b>ip access-list</b> | Assigns an ID to an access list and enters access list configuration mode.   |
| <b>ip http server</b> | Enables the HTTP 1.1 server, including the Cisco web browser user interface. |

## ip radius source-interface

To force RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets, use the **ip radius source-interface** command in global configuration mode. To prevent RADIUS from using the IP address of a specified interface for all outgoing RADIUS packets, use the no form of this command.

**ip radius source-interface** *interface-name* [**vrf** *vrf-name*]  
**no ip radius source-interface**

|                           |                            |   |
|---------------------------|----------------------------|---|
| <b>Syntax Description</b> | <i>interface-name</i>      | Name of the interface that RADIUS uses for all of its outgoing packets. |
|                           | <b>vrf</b> <i>vrf-name</i> | (Optional) Per virtual route forwarding (VRF) configuration.            |

**Command Default** No default behavior or values.

**Command Modes** Global configuration (config)

| <b>Command History</b> | <b>Release</b>              | <b>Modification</b>          |
|------------------------|-----------------------------|------------------------------|
|                        | Cisco IOS XE Everest 16.6.1 | This command was introduced. |

**Usage Guidelines** Use this command to set the IP address of an interface to be used as the source address for all outgoing RADIUS packets. The IP address is used as long as the interface is in the *up* state. The RADIUS server can use one IP address entry for every network access client instead of maintaining a list of IP addresses. Radius uses the IP address of the interface that it is associated to, regardless of whether the interface is in the *up* or *down* state.

The **ip radius source-interface** command is especially useful in cases where the router has many interfaces and you want to ensure that all RADIUS packets from a particular router have the same IP address.

The specified interface should have a valid IP address and should be in the *up* state for a valid configuration. If the specified interface does not have a valid IP address or is in the *down* state, RADIUS selects a local IP that corresponds to the best possible route to the AAA server. To avoid this, add a valid IP address to the interface or bring the interface to the *up* state.

Use the **vrf** *vrf-name* keyword and argument to configure this command per VRF, which allows multiple disjointed routing or forwarding tables, where the routes of one user have no correlation with the routes of another user.

### Examples

The following example shows how to configure RADIUS to use the IP address of interface s2 for all outgoing RADIUS packets:

```
ip radius source-interface s2
```

The following example shows how to configure RADIUS to use the IP address of interface Ethernet0 for VRF definition:

```
ip radius source-interface Ethernet0 vrf vrfl
```

# ip source binding

To add a static IP source binding entry, use the **ip source binding** command. Use the **no** form of this command to delete a static IP source binding entry

**ip source binding** *mac-address* **vlan** *vlan-id* *ip-address* **interface** *interface-id*  
**no ip source binding** *mac-address* **vlan** *vlan-id* *ip-address* **interface** *interface-id*

|                           |                                       |   |
|---------------------------|---------------------------------------|---|
| <b>Syntax Description</b> | <i>mac-address</i>                    | Binding MAC address.  |
|                           | <b>vlan</b> <i>vlan-id</i>            | Specifies the Layer 2 VLAN identification; valid values are from 1 to 4094. |
|                           | <i>ip-address</i>                     | Binding IP address.   |
|                           | <b>interface</b> <i>interface-id</i>  | ID of the physical interface.   |
| <b>Command Default</b>    | No IP source bindings are configured. |   |
| <b>Command Modes</b>      | Global configuration (config)         |   |
| <b>Command History</b>    | <b>Release</b>                        | <b>Modification</b>   |
|                           | Cisco IOS XE Everest 16.6.1           | This command was introduced.  |

**Usage Guidelines**

You can use this command to add a static IP source binding entry only.

The **no** format deletes the corresponding IP source binding entry. It requires the exact match of all required parameter in order for the deletion to be successful. Note that each static IP binding entry is keyed by a MAC address and a VLAN number. If the command contains the existing MAC address and VLAN number, the existing binding entry is updated with the new parameters instead of creating a separate binding entry.

This example shows how to add a static IP source binding entry:

```
Device> enable
Device# configure terminal
Device(config) ip source binding 0100.0230.0002 vlan 11 10.0.0.4 interface
gigabitethernet1/0/1
Device(config)# exit
```

# ip ssh source-interface

To specify the IP address of an interface as the source address for a Secure Shell (SSH) client device, use the **ip ssh source-interface** command in global configuration mode. To remove the IP address as the source address, use the **no** form of this command.

**ip ssh source-interface** *interface*  
**no ip ssh source-interface** *interface*

## Syntax Description

|                  |   |
|------------------|---|
| <i>interface</i> | The interface whose address is used as the source address for the SSH client. |
|------------------|---|

## Command Default

The address of the closest interface to the destination is used as the source address (the closest interface is the output interface through which the SSH packet is sent).

## Command Modes

Global configuration (config)

## Command History

| Release                        | Modification                 |
|--------------------------------|------------------------------|
| Cisco IOS XE Gibraltar 16.10.1 | This command was introduced. |
| Cisco IOS XE Gibraltar 16.11.1 |                              |

## Usage Guidelines

By specifying this command, you can force the SSH client to use the IP address of the source interface as the source address.

## Examples

In the following example, the IP address assigned to GigabitEthernet interface 1/0/1 is used as the source address for the SSH client:

```
Device> enable
Device# configure terminal
Device(config)# ip ssh source-interface GigabitEthernet 1/0/1
Device(config)# exit
```

# ip verify source

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

**ip verify source** [**mac-check**] [**tracking**]  
**no ip verify source**

|                  |  |
|------------------|--|
| <b>mac-check</b> | (Optional) Enables IP source guard with MAC address verification.                  |
| <b>tracking</b>  | (Optional) Enables IP port security to learn static IP address learning on a port. |

**Command Default** IP source guard is disabled.

**Command Modes** Interface configuration (config-if)

| <b>Command History</b> | <b>Release</b>              | <b>Modification</b>          |
|------------------------|-----------------------------|------------------------------|
|                        | Cisco IOS XE Everest 16.6.1 | This command was introduced. |

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

To enable IP source guard with source IP address filtering and MAC address verification, use the **ip verify source mac-check** interface configuration command.

## Examples

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

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip verify source
Device(config-if)# end
```

This example shows how to enable IP source guard with MAC address verification:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip verify source mac-check
Device(config-if)# end
```

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

# 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

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

## Command Default

No IPv6 access list is defined.

## Command Modes

Global configuration (config)

## Command History

| Release                     | Modification                 |
|-----------------------------|------------------------------|
| Cisco IOS XE Everest 16.6.1 | 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. 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> enable
Device# configure terminal
Device(config)# ipv6 access-list list1
Device(config-ipv6-acl)# end
```

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 from GigabitEthernet interface 0/1/2. 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> enable
Device# configure terminal
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 gigabitethernet 0/1/2
Device(config-if)# ipv6 traffic-filter list2 out
Device(config-if)# end
```

# ipv6 snooping policy

To configure an IPv6 snooping policy and enter IPv6 snooping configuration mode, use the **ipv6 snooping policy** command in global configuration mode. To delete an IPv6 snooping policy, use the **no** form of this command.

**ipv6 snooping policy** *snooping-policy*  
**no ipv6 snooping policy** *snooping-policy*

|                           |  |                              |
|---------------------------|--|------------------------------|
| <b>Syntax Description</b> | <i>snooping-policy</i> User-defined name of the snooping policy. The policy name can be a symbolic string (such as Engineering) or an integer (such as 0).   |                              |
| <b>Command Default</b>    | An IPv6 snooping policy is not configured.   |                              |
| <b>Command Modes</b>      | Global configuration (config)  |                              |
| <b>Command History</b>    | <b>Release</b>   | <b>Modification</b>          |
|                           | Cisco IOS XE Everest 16.6.1  | This command was introduced. |
| <b>Usage Guidelines</b>   | <p>Use the <b>ipv6 snooping policy</b> command to create an IPv6 snooping policy. When the <b>ipv6 snooping policy</b> command is enabled, the configuration mode changes to IPv6 snooping configuration mode. In this mode, the administrator can configure the following IPv6 first-hop security commands:</p> <ul style="list-style-type: none"> <li>• The <b>device-role</b> command specifies the role of the device attached to the port.</li> <li>• The <b>limit address-count</b> <i>maximum</i> command limits the number of IPv6 addresses allowed to be used on the port.</li> <li>• The <b>protocol</b> command specifies that addresses should be gleaned with Dynamic Host Configuration Protocol (DHCP) or Neighbor Discovery Protocol (NDP).</li> <li>• The <b>security-level</b> command specifies the level of security enforced.</li> <li>• The <b>tracking</b> command overrides the default tracking policy on a port.</li> <li>• The <b>trusted-port</b> command configures a port to become a trusted port; that is, limited or no verification is performed when messages are received.</li> </ul> |                              |

This example shows how to configure an IPv6 snooping policy:

```
Device> enable
Device# configure terminal
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# end
```

# key chain macsec

To configure a MACsec key chain name on a device interface to fetch a Pre Shared Key (PSK), use the **key chain macsec** command in global configuration mode. To disable it, use the **no** form of this command.

**key chain** *name* **macsec**  
**no key chain** *name* [**macsec** ]

| <b>Syntax Description</b>   | <i>name</i> Name of a key chain to be used to get keys.  |         |              |                             |                              |
|-----------------------------|--|---------|--------------|-----------------------------|------------------------------|
| <b>Command Default</b>      | Key chain macsec is disabled.  |         |              |                             |                              |
| <b>Command Modes</b>        | Global configuration (config)  |         |              |                             |                              |
| <b>Command History</b>      | <table> <tr> <th>Release</th><th>Modification</th></tr> <tr> <td>Cisco IOS XE Everest 16.6.1</td><td>This command was introduced.</td></tr> </table> | Release | Modification | Cisco IOS XE Everest 16.6.1 | This command was introduced. |
| Release                     | Modification   |         |              |                             |                              |
| Cisco IOS XE Everest 16.6.1 | This command was introduced.   |         |              |                             |                              |

This example shows how to configure MACsec key chain to fetch a 128-bit Pre Shared Key (PSK):

```
Device> enable
Device# configure terminal
Device(config)# key chain kc1 macsec
Device(config-keychain-macsec)# key 1000
Device(config-keychain-macsec)# cryptographic-algorithm aes-128-cmac
Device(config-keychain-macsec-key)# key-string fb63e0269e2768c49bab8ee9a5c2258f
Device(config-keychain-macsec-key)# end
Device#
```

This example shows how to configure MACsec key chain to fetch a 256-bit Pre Shared Key (PSK):

```
Device> enable
Device# configure terminal
Device(config)# key chain kc1 macsec
Device(config-keychain-macsec)# key 2000
Device(config-keychain-macsec)# cryptographic-algorithm aes-256-cmac
Device(config-keychain-macsec-key)# key-string c865632acb269022447c417504a1b
f5db1c296449b52627ba01f2ba2574c2878
Device(config-keychain-macsec-key)# end
Device#
```

# key config-key password-encrypt

To store a type 6 encryption key in private NVRAM, use the **key config-key password-encrypt** command in global configuration mode. To disable the encryption, use the **no** form of this command.

**key config-key password-encrypt** [*text*]  
**no key config-key password-encrypt** [*text*]

## Syntax Description

*text* (Optional) Password or master key.

### Note

We recommended that you do not use the *text* argument, and instead use interactive mode (using the **Enter** key after you enter the **key config-key password-encrypt** command) so that the preshared key is not printed anywhere and, therefore, cannot be seen.

## Command Default

Type 6 password encryption key is not stored in private NVRAM.

## Command Modes

Global configuration (config)

## Command History

### Release

Cisco IOS XE Everest 16.6.1

### Modifica

This com  
introduce

## Usage Guidelines

You can securely store plain text passwords in type 6 format in NVRAM using a CLI. Type 6 passwords are encrypted. Although the encrypted passwords can be seen or retrieved, it is difficult to decrypt them to find out the actual password. Use the **key config-key password-encrypt** command along with the **password encryption aes** command to configure and enable the password (symmetric cipher Advanced Encryption Standard [AES] is used to encrypt the keys). The password (key) configured using the **key config-key password-encrypt** command is the master encryption key that is used to encrypt all other keys in the device.

If you configure the **password encryption aes** command without configuring the **key config-key password-encrypt** command, the following message is displayed at startup or during a nonvolatile generation (NVGEN) process, such as when the **show running-config** or **copy running-config startup-config** commands are configured:

```
"Can not encrypt password. Please configure a configuration-key with 'key config-key'"
```

### Changing a Password

If the password (master key) is changed or reencrypted, use the **key config-key password-encrypt** command for the list registry to pass the old key and the new key to the application modules that are using type 6 encryption.

### Deleting a Password

If the master key that was configured using the **key config-key password-encrypt** command is deleted from the system, a warning is displayed (and a confirm prompt is issued) stating that all type 6 passwords will become useless. As a security measure, after the passwords are encrypted, they will never be decrypted in the Cisco IOS software. However, passwords can be re-encrypted, as explained in the previous paragraph.

**Caution**

If the password that is configured using the **key config-key password-encrypt** command is lost, it cannot be recovered. We, therefore, recommend that you store the password in a safe location.

### Unconfiguring Password Encryption

If you unconfigure password encryption using the **no password encryption aes** command, all the existing type 6 passwords are left unchanged, and as long as the password (master key) that was configured using the **key config-key password-encrypt** command exists, the type 6 passwords will be decrypted as and when required by the application.

### Storing Passwords

Because no one can *read* the password (configured using the **key config-key password-encrypt** command), there is no way that the password can be retrieved from the device. Existing management stations cannot *know* what it is unless the stations are enhanced to include this key somewhere, in which case, the password needs to be stored securely within the management system. If configurations are stored using TFTP, the configurations are not standalone, meaning that they cannot be loaded onto a device. Before or after the configurations are loaded onto a device, the password must be manually added (using the **key config-key password-encrypt** command). The password can be manually added to the stored configuration. However we do not recommend this because adding the password manually allows anyone to decrypt all the passwords in that configuration.

### Configuring New or Unknown Passwords

If you enter or cut and paste ciphertext that does not match the master key, or if there is no master key, the ciphertext is accepted or saved, but an alert message is displayed:

```
"ciphertext>[for username bar] is incompatible with the configured master key."
```

If a new master key is configured, all plain keys are encrypted and made type 6 keys. The existing type 6 keys are not encrypted. The existing type 6 keys are left as is.

If the old master key is lost or is unknown, you have the option of deleting the master key using the **no key config-key password-encrypt** command. Deleting the master key causes the existing encrypted passwords to remain encrypted in the device configuration. The passwords cannot be decrypted.

### Examples

The following example shows how a type 6 encryption key is stored in NVRAM:

```
Device> enable
Device# configure terminal
Device (config)# key config-key password-encrypt
```

### Related Commands

| Command                        | Description                  |
|--------------------------------|------------------------------|
| <b>password encryption aes</b> | Enables a type 6 encrypted p |

# key-server

To configure MKA key-server options, use the **key-server** command in MKA-policy configuration mode. To disable MKA key-server options, use the **no** form of this command.

**key-server priority** *value*

**no key-server priority**

## Syntax Description

**priority** *value*

Specifies the priority value of the MKA key-server.

## Command Default

MKA key-server is disabled.

## Command Modes

MKA-policy configuration (config-mka-policy)

## Command History

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

## Examples

The following example shows how to configure the MKA key-server:

```
Device> enable
Device# configure terminal
Device(config)# mka policy 2
Device(config-mka-policy)# key-server priority 33
```

## Related Commands

| Command                          | Description  |
|----------------------------------|--|
| <b>mka policy</b>                | Configures an MKA policy.                                      |
| <b>confidentiality-offset</b>    | Sets the confidentiality offset for MACsec operations.         |
| <b>delay-protection</b>          | Configures MKA to use delay protection in sending MKPDU.       |
| <b>include-icv-indicator</b>     | Includes ICV indicator in MKPDU.                               |
| <b>macsec-cipher-suite</b>       | Configures cipher suite for deriving SAK)                      |
| <b>sak-rekey</b>                 | Configures the SAK rekey interval.                             |
| <b>send-secure-announcements</b> | Configures MKA to send secure announcements in sending MKPDUs. |
| <b>ssci-based-on-sci</b>         | Computes SSCI based on the SCI.                                |
| <b>use-updated-eth-header</b>    | Uses the updated Ethernet header for ICV calculation.          |

# limit address-count

To limit the number of IPv6 addresses allowed to be used on the port, use the **limit address-count** command in Neighbor Discovery Protocol (NDP) inspection policy configuration mode or IPv6 snooping configuration mode. To return to the default, use the **no** form of this command.

**limit address-count** *maximum*  
**no limit address-count**

|                           |   |                              |
|---------------------------|---|------------------------------|
| <b>Syntax Description</b> | <i>maximum</i> The number of addresses allowed on the port. The range is from 1 to 10000.   |                              |
| <b>Command Default</b>    | The default is no limit.  |                              |
| <b>Command Modes</b>      | IPv6 snooping configuration (config-ipv6-snooping)<br>ND inspection policy configuration (config-nd-inspection)   |                              |
| <b>Command History</b>    | <b>Release</b>  | <b>Modification</b>          |
|                           | Cisco IOS XE Everest 16.6.1   | This command was introduced. |
| <b>Usage Guidelines</b>   | <p>The <b>limit address-count</b> command limits the number of IPv6 addresses allowed to be used on the port on which the policy is applied. Limiting the number of IPv6 addresses on a port helps limit the binding table size. The range is from 1 to 10000.</p> <p>This example shows how to define an NDP policy name as policy1, and limit the number of IPv6 addresses allowed on the port to 25:</p> <pre>Device&gt; enable Device# configure terminal Device(config)# ipv6 nd inspection policy policy1 Device(config-nd-inspection)# limit address-count 25 Device(config-nd-inspection)# end</pre> <p>This example shows how to define an IPv6 snooping policy name as policy1, and limit the number of IPv6 addresses allowed on the port to 25:</p> <pre>Device&gt; enable Device# configure terminal Device(config)# ipv6 snooping policy policy1 Device(config-ipv6-snooping)# limit address-count 25 Device(config-ipv6-snooping)# end</pre> |                              |

# mab logging verbose

To filter detailed information from MAC authentication bypass (MAB) system messages, use the **mab logging verbose** command in global configuration mode. Use the no form of this command to disable logging MAB system messages.

**mab logging verbose**  
**no mab logging verbose**

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

**Command Default** Detailed logging of system messages is not enabled.

**Command Modes** Global configuration (config)

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

**Usage Guidelines** This command filters details, such as anticipated success, from MAC authentication bypass (MAB) system messages. Failure messages are not filtered.

To filter verbose MAB system messages:

```
Device> enable
Device# configure terminal
Device(config)# mab logging verbose
Device(config)# exit
```

You can verify your settings by entering the **show running-config** command.

| Related Commands | Command                               | Description   |
|------------------|---------------------------------------|---|
|                  | <b>authentication logging verbose</b> | Filters details from authentication system messages.                  |
|                  | <b>dot1x logging verbose</b>          | Filters details from 802.1x system messages.                          |
|                  | <b>mab logging verbose</b>            | Filters details from MAC authentication bypass (MAB) system messages. |



## mab request format attribute 32

To enable VLAN ID-based MAC authentication on a device, use the **mab request format attribute 32 vlan access-vlan** command in global configuration mode. To return to the default setting, use the **no** form of this command.

```
mab request format attribute 32 vlan access-vlan
no mab request format attribute 32 vlan access-vlan
```

### Syntax Description

This command has no arguments or keywords.

### Command Default

VLAN-ID based MAC authentication is disabled.

### Command Modes

Global configuration (config)

### Command History

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

### Usage Guidelines

Use this command to allow a RADIUS server to authenticate a new user based on the host MAC address and VLAN. Use this feature on networks with the Microsoft IAS RADIUS server. The Cisco ACS ignores this command.

This example shows how to enable VLAN-ID based MAC authentication on a device:

```
Device> enable
Device# configure terminal
Device(config)# mab request format attribute 32 vlan access-vlan
Device(config)# exit
```

### Related Commands

| Command                            | Description  |
|------------------------------------|--|
| <b>authentication event</b>        | Sets the action for specific authentication events.  |
| <b>authentication fallback</b>     | Configures a port to use web authentication as a fallback method that do not support IEEE 802.1x authentication. |
| <b>authentication host-mode</b>    | Sets the authorization manager mode on a port.   |
| <b>authentication open</b>         | Enables or disables open access on a port.   |
| <b>authentication order</b>        | Sets the order of authentication methods used on a port.   |
| <b>authentication periodic</b>     | Enables or disables reauthentication on a port.  |
| <b>authentication port-control</b> | Enables manual control of the port authorization state.  |
| <b>authentication priority</b>     | Adds an authentication method to the port-priority list.   |
| <b>authentication timer</b>        | Configures the timeout and reauthentication parameters for a 802.1x-enabled port.                                |

| Command                         | Description   |
|---------------------------------|---|
| <b>authentication violation</b> | Configures the violation modes that occur when a new device connects to a port or when a new device connects to a port with the maximum number of devices already connected to that port. |
| <b>mab</b>                      | Enables MAC-based authentication on a port.   |
| <b>mab eap</b>                  | Configures a port to use the Extensible Authentication Protocol (EAP).  |
| <b>show authentication</b>      | Displays information about authentication manager events on the port.   |

# macsec-cipher-suite

To configure cipher suite for deriving Security Association Key (SAK), use the **macsec-cipher-suite** command in MKA-policy configuration mode. To disable cipher suite for SAK, use the **no** form of this command.

**macsec-cipher-suite** {gcm-aes-128 | gcm-aes-256 }  
**no macsec-cipher-suite** {gcm-aes-128 | gcm-aes-256 }

## Syntax Description

**gcm-aes-128** Configures cipher suite for deriving SAK with 128-bit encryption.

**gcm-aes-256** Configures cipher suite for deriving SAK with 256-bit encryption.

## Command Default

GCM-AES-128 encryption is enabled.

## Command Modes

MKA-policy configuration (config-mka-policy)

## Command History

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

## Usage Guidelines

If the device supports both GCM-AES-128 and GCM-AES-256 ciphers, it is highly recommended to define and use a user-defined MKA policy to include both or only 256 bits cipher, based on your requirements..

## Examples

The following example shows how to configure MACsec cipher suite for deriving SAK with 256-bit encryption:

```
Device> enable
Device# configure terminal
Device(config)# mka policy 2
Device(config-mka-policy)# macsec-cipher-suite gcm-aes-256
```

## Related Commands

| Command                          | Description  |
|----------------------------------|--|
| <b>mka policy</b>                | Configures an MKA policy.                                      |
| <b>confidentiality-offset</b>    | Sets the confidentiality offset for MACsec operations.         |
| <b>delay-protection</b>          | Configures MKA to use delay protection in sending MKPDU.       |
| <b>include-icv-indicator</b>     | Includes ICV indicator in MKPDU.                               |
| <b>key-server</b>                | Configures MKA key-server options.                             |
| <b>sak-rekey</b>                 | Configures the SAK rekey interval.                             |
| <b>send-secure-announcements</b> | Configures MKA to send secure announcements in sending MKPDUs. |
| <b>ssci-based-on-sci</b>         | Computes SSCI based on the SCI.                                |

| Command                       | Description   |
|-------------------------------|---|
| <b>use-updated-eth-header</b> | Uses the updated Ethernet header for ICV calculation. |

## macsec network-link

To enable MACsec Key Agreement protocol (MKA) configuration on the uplink interfaces, use the **macsec network-link** command in interface configuration mode. To disable it, use the **no** form of this command.

**macsec network-link**

**no macsec network-link**

|                           |   |                              |
|---------------------------|---|------------------------------|
| <b>Syntax Description</b> | <b>macsec network-link</b> Enables MKA MACsec configuration on device interfaces using EAP-TLS authentication protocol. |                              |
| <b>Command Default</b>    | MACsec network-link is disabled.  |                              |
| <b>Command Modes</b>      | Interface configuration (config-if)   |                              |
| <b>Command History</b>    | <b>Release</b>  | <b>Modification</b>          |
|                           | Cisco IOS XE Everest 16.6.1   | This command was introduced. |

This example shows how to configure MACsec MKA on an interface using the EAP-TLS authentication protocol:

```
Device> enable
Device# configure terminal
Device(config)# interface GigabitEthernet 1/0/20
Device(config-if)# macsec network-link
Device(config-if)# end
Device#
```

# 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. To remove the match parameters, use the **no** form of this command.

```
match {ip address {namenumber} [{namenumber}] [{namenumber}]... | ipv6 address {namenumber}
[{namenumber}] [{namenumber}]... | mac address {name} [{name}] [{name}]... }
no match {ip address {namenumber} [{namenumber}] [{namenumber}]... | ipv6 address
{namenumber} [{namenumber}] [{namenumber}]... | mac address {name} [{name}] [{name}]... }
```

## Syntax Description

|                     |  |
|---------------------|--|
| <b>ip address</b>   | Sets the access map to match packets against an IP address access list.                            |
| <b>ipv6 address</b> | Sets the access map to match packets against an IPv6 address access list.                          |
| <b>mac address</b>  | Sets the access map to match packets against a MAC address access list.                            |
| <i>name</i>         | Name of the access list to match packets against.  |
| <i>number</i>       | 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 (config-access-map)

## Command History

| Release                     | Modification                 |
|-----------------------------|------------------------------|
| Cisco IOS XE Everest 16.6.1 | 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.

## 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> enable
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  
Device(config)# exit
```

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

# mka pre-shared-key

To configure MACsec Key Agreement (MKA) MACsec on a device interface using a Pre Shared Key (PSK), use the **mka pre-shared-key key-chain** *key-chain name* command in interface configuration mode. To disable it, use the **no** form of this command.

```
mka pre-shared-key key-chain key-chain-name
no mka pre-shared-key key-chain key-chain-name
```

| Syntax Description | mka pre-shared-key key-chain Enables MACsec MKA configuration on device interfaces using a PSK. |                              |
|--------------------|---|------------------------------|
| Command Default    | MKA pre-shared-key is disabled.   |                              |
| Command Modes      | Interface configuration (config-if)   |                              |
| Command History    | Release   | Modification                 |
|                    | Cisco IOS XE Everest 16.6.1   | This command was introduced. |

This example shows how to configure MKA MACsec on an interface using a PSK:

```
Device> enable
Device# configure terminal
Device(config)# interface Gigabitethernet 1/0/20
Device(config-if)# mka pre-shared-key key-chain kcl
Device(config-if)# end
Device#
```



# mka suppress syslogs sak-rekey

To suppress MACsec Key Agreement (MKA) secure association key (SAK) rekey messages during logging, use the **mka suppress syslogs sak-rekey** command in global configuration mode. To enable MKA SAK rekey message logging, use the **no** form of this command.

**mka suppress syslogs sak-rekey**  
**no mka suppress syslogs sak-rekey**

This command has no arguments or keywords.

## Command Default

All MKA SAK syslog messages are displayed on the console.

## Command Modes

Global configuration (config)

## Command History

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

## Usage Guidelines

MKA SAK syslogs are continuously generated at every rekey interval, and when MKA is configured on multiple interfaces, the amount of syslog generated is too high. Use this command to suppress the MKA SAK syslogs.

## Example

The following example shows how to suppress MKA SAK syslog logging:

```
Device> enable
Device# configure terminal
Device(config)# mka suppress syslogs sak-rekey
```

# password encryption aes

To enable a type 6 encrypted preshared key, use the **password encryption aes** command in global configuration mode. To disable password encryption, use the **no** form of this command.

**password encryption aes**  
**no password encryption aes**

|                           |  |   |
|---------------------------|--|---|
| <b>Syntax Description</b> | This command has no arguments or keywords. |   |
| <b>Command Default</b>    | Preshared keys are not encrypted.          |   |
| <b>Command Modes</b>      | Global configuration (config)              |   |
| <b>Command History</b>    | <b>Release</b>                             | <b>Modification</b>   |
|                           | Cisco IOS XE Everest 16.6.1                | This command was introduced in Cisco IOS XE Everest 16.6.1. |

**Usage Guidelines**

You can securely store plain text passwords in type 6 format in NVRAM using a CLI. Type 6 passwords are encrypted. Although the encrypted passwords can be seen or retrieved, it is difficult to decrypt them to find out the actual password. Use the **key config-key password-encrypt** command along with the **password encryption aes** command to configure and enable the password (symmetric cipher Advanced Encryption Standard [AES] is used to encrypt the keys). The password (key) that is configured using the **key config-key password-encrypt** command is the master encryption key that is used to encrypt all other keys in the router.

If you configure the **password encryption aes** command without configuring the **key config-key password-encrypt** command, the following message is displayed at startup or during a nonvolatile generation (NVGEN) process, such as when the **show running-config** or **copy running-config startup-config** commands are run:

```
"Can not encrypt password. Please configure a configuration-key with 'key config-key'"
```

## Changing a Password

If the password (master key) is changed or re-encrypted using the **key config-key password-encrypt** command, the list registry passes the old key and the new key to the application modules that are using type 6 encryption.

## Deleting a Password

If the master key that was configured using the **key config-key password-encrypt** command is deleted from the system, a warning is displayed (and a confirm prompt is issued) that states that all type 6 passwords will no longer be applicable. As a security measure, after the passwords are encrypted, they will never be decrypted in the Cisco IOS software. However, passwords can be re-encrypted as explained in the previous paragraph.



**Caution** If a password that is configured using the **key config-key password-encrypt** command is lost, it cannot be recovered. Therefore, the password should be stored in a safe location.

## Unconfiguring Password Encryption

If you unconfigure password encryption using the **no password encryption aes** command, all the existing type 6 passwords are left unchanged. As long as the password (master key) that was configured using the **key config-key password-encrypt** command exists, the type 6 passwords are decrypted as and when required by the application.

### Storing Passwords

Because no one can *read* the password (configured using the **key config-key password-encrypt** command), there is no way that the password can be retrieved from the router. Existing management stations cannot *know* what it is unless the stations are enhanced to include this key somewhere. Therefore, the password needs to be stored securely within the management system. If configurations are stored using TFTP, the configurations are not standalone, meaning that they cannot be loaded onto a router. Before or after the configurations are loaded onto a router, the password must be manually added (using the **key config-key password-encrypt** command). The password can be manually added to the stored configuration, but we do not recommend this because adding the password manually allows anyone to decrypt all the passwords in that configuration.

### Configuring New or Unknown Passwords

If you enter or cut and paste ciphertext that does not match the master key, or if there is no master key, the ciphertext is accepted or saved, but the following alert message is displayed:

```
"ciphertext>[for username bar>] is incompatible with the configured master key."
```

If a new master key is configured, all the plain keys are encrypted and converted to type 6 keys. The existing type 6 keys are not encrypted. The existing type 6 keys are left as is.

If the old master key is lost or unknown, you have the option of deleting the master key using the **no key config-key password-encrypt** command. This causes the existing encrypted passwords to remain encrypted in the router configuration. The passwords will not be decrypted.

### Examples

The following example shows how a type 6 encrypted preshared key is enabled:

```
Device> enable
Device# configure terminal
Device (config)# password encryption aes
```

### Related Commands

| Command                                | Description                    |
|--|--------------------------------|
| <b>key config-key password-encrypt</b> | Stores a type 6 encryption key |

## permit (MAC access-list configuration)

To allow non-IP traffic to be forwarded if the conditions are matched, use the **permit** command in MAC access-list configuration mode. To remove a permit condition from the extended MAC access list, use the **no** form of this command.

```
{permit {any | hostsrc-MAC-addr | src-MAC-addr mask} {any | hostdst-MAC-addr |  
dst-MAC-addr mask} [type mask | aarp | amber | appletalk | dec-spanning | decnet-iv |  
diagnostic | dsm | etype-6000 | etype-8042 | lat | lavr-sca | lsaplsap mask | mop-console  
| mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-idp] [coscos]  
nopermit {any | host src-MAC-addr | src-MAC-addr mask} {any | host dst-MAC-addr |  
dst-MAC-addr mask} [type mask | aarp | amber | appletalk | dec-spanning | decnet-iv |  
diagnostic | dsm | etype-6000 | etype-8042 | lat | lavr-sca | lsap lsap mask | mop-console  
| mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-idp] [coscos]
```

### Syntax Description

|  |  |
|--|--|
| <b>any</b>   | Denies any source or destination MAC address.  |
| <b>host</b> <i>src-MAC-addr</i>   <i>src-MAC-addr mask</i> | Specifies a host MAC address and optional subnet mask. If the defined address, non-IP traffic from that address is denied.   |
| <b>host</b> <i>dst-MAC-addr</i>   <i>dst-MAC-addr mask</i> | Specifies a destination MAC address and optional subnet mask. If the defined address matches the defined address, non-IP traffic to that address is denied.  |
| <i>type mask</i>   | (Optional) Specifies the EtherType number of a packet to identify the protocol of the packet. <ul style="list-style-type: none"> <li><i>type</i> is 0 to 65535, specified in hexadecimal.</li> <li><i>mask</i> is a mask of don't care bits applied to the EtherType.</li> </ul> |
| <b>aarp</b>  | (Optional) Specifies EtherType AppleTalk Address Resolution Protocol to a network address.   |
| <b>amber</b>   | (Optional) Specifies EtherType DEC-Amber.  |
| <b>appletalk</b>   | (Optional) Specifies EtherType AppleTalk/EtherTalk.  |
| <b>dec-spanning</b>  | (Optional) Specifies EtherType Digital Equipment Corporation Spanning Tree Protocol.   |
| <b>decnet-iv</b>   | (Optional) Specifies EtherType DECnet Phase IV protocol.   |
| <b>diagnostic</b>  | (Optional) Specifies EtherType DEC-Diagnostic.   |
| <b>dsm</b>   | (Optional) Specifies EtherType DEC-DSM.  |
| <b>etype-6000</b>  | (Optional) Specifies EtherType 0x6000.   |
| <b>etype-8042</b>  | (Optional) Specifies EtherType 0x8042.   |
| <b>lat</b>   | (Optional) Specifies EtherType DEC-LAT.  |
| <b>lavr-sca</b>  | (Optional) Specifies EtherType DEC-LAVC-SCA.   |

|                                     |  |
|-------------------------------------|--|
| <b>lsap</b> <i>lsap-number mask</i> | (Optional) Specifies the LSAP number (0 to 65535) of the protocol of the packet.<br><br>The <i>mask</i> is a mask of don't care bits applied to the LSAP number. |
| <b>mop-console</b>                  | (Optional) Specifies EtherType DEC-MOP Remote Console.   |
| <b>mop-dump</b>                     | (Optional) Specifies EtherType DEC-MOP Dump.   |
| <b>msdos</b>                        | (Optional) Specifies EtherType DEC-MSDOS.  |
| <b>mumps</b>                        | (Optional) Specifies EtherType DEC-MUMPS.  |
| <b>netbios</b>                      | (Optional) Specifies EtherType DEC- Network Basic Input/Output System.   |
| <b>vines-echo</b>                   | (Optional) Specifies EtherType Virtual Integrated Network Environment.   |
| <b>vines-ip</b>                     | (Optional) Specifies EtherType VINES IP.   |
| <b>xns-idp</b>                      | (Optional) Specifies EtherType Xerox Network System.   |
| <b>cos</b> <i>cos</i>               | (Optional) Specifies an arbitrary class of service (CoS). CoS can be performed only in hardware. A warning message is displayed if CoS is not supported.         |

**Command Default**

This command has no defaults. However, the default action for a MAC-named ACL is to deny.

**Command Modes**

MAC-access list configuration

**Command History**

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

**Usage Guidelines**

Though visible in the command-line help strings, **appletalk** is not supported as a matching condition.

You enter MAC access-list configuration mode by using the **mac access-list extended** global configuration command.

If you use the **host** keyword, you cannot enter an address mask; if you do not use the **any** or **host** keywords, you must enter an address mask.

After an access control entry (ACE) is added to an access control list, an implied **deny-any-any** condition exists at the end of the list. That is, if there are no matches, the packets are denied. However, before the first ACE is added, the list permits all packets.

To filter IPX traffic, you use the *type mask* or **lsap lsap mask** keywords, depending on the type of IPX encapsulation being used. Filter criteria for IPX encapsulation types as specified in Novell terminology and Cisco IOS XE terminology are listed in the following table.

**Table 3: IPX Filtering Criteria**

| IPX Encapsulation Type |             | Filter Criterion |
|------------------------|-------------|------------------|
| Cisco IOS Name         | Novell Name |                  |
| arpa                   | Ethernet II | EtherType 0x8137 |

| IPX Encapsulation Type |                | Filter Criterion |
|------------------------|----------------|------------------|
| Cisco IOS Name         | Novell Name    |                  |
| snap                   | Ethernet-snap  | EtherType 0x8137 |
| sap                    | Ethernet 802.2 | LSAP 0xE0E0      |
| novell-ether           | Ethernet 802.3 | LSAP 0xFFFF      |

This example shows how to define the MAC-named extended access list to allow NetBIOS traffic from any source to MAC address 00c0.00a0.03fa. Traffic matching this list is allowed.

```
Device> enable
Device# configure terminal
Device(config)# mac access-list extended
Device(config-ext-macl)# permit any host 00c0.00a0.03fa netbios
Device(config-ext-macl)# end
```

This example shows how to remove the permit condition from the MAC-named extended access list:

```
Device> enable
Device# configure terminal
Device(config)# mac access-list extended
Device(config-ext-macl)# no permit any 00c0.00a0.03fa 0000.0000.0000 netbios
Device(config-ext-macl)# end
```

This example permits all packets with EtherType 0x4321:

```
Device> enable
Device# configure terminal
Device(config)# mac access-list extended
Device(config-ext-macl)# permit any any 0x4321 0
Device(config-ext-macl)# end
```

You can verify your settings by entering the **show access-lists** command.

## Related Commands

| Command                         | Description                                 |
|---------------------------------|---|
| <b>deny</b>                     | Denies from the MAC non-IP traffic to be fo |
| <b>mac access-list extended</b> | Creates an access list traffic.             |
| <b>show access-lists</b>        | Displays access contr                       |

# protocol (IPv6 snooping)

s

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 in IPv6 snooping configuration mode. To disable address gleaned with DHCP or NDP, use the **no** form of the command.

```
protocol {dhcp | ndp}
no protocol {dhcp | ndp}
```

|                           |   |   |
|---------------------------|---|---|
| <b>Syntax Description</b> | <b>dhcp</b>   | Specifies that addresses should be gleaned in Dynamic Host Configuration Protocol (DHCP) packets. |
|                           | <b>ndp</b>  | Specifies that addresses should be gleaned in Neighbor Discovery Protocol (NDP) packets.          |
| <b>Command Default</b>    | Snooping and recovery are attempted using both DHCP and NDP.  |   |
| <b>Command Modes</b>      | IPv6 snooping configuration mode (config-ipv6-snooping)   |   |
| <b>Command History</b>    | <b>Release</b>  | <b>Modification</b>   |
|                           | Cisco IOS XE Everest 16.6.1   | This command was introduced.  |
| <b>Usage Guidelines</b>   | <p>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.</p> <ul style="list-style-type: none"><li>• Using the <b>no protocol {dhcp   ndp}</b> command indicates that a protocol will not be used for snooping or gleaning.</li><li>• If the <b>no protocol dhcp</b> command is used, DHCP can still be used for binding table recovery.</li><li>• Data glean can recover with DHCP and NDP, though destination guard will only recovery through DHCP.</li></ul> |   |

This example shows how to define an IPv6 snooping policy name as policy1, and configure the port to use DHCP to glean addresses:

```
Device> enable
Device# configure terminal
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# protocol dhcp
Device(config-ipv6-snooping)# end
```

# radius server

To configure the RADIUS server parameters, including the RADIUS accounting and authentication, use the **radius server** command in global configuration mode. Use the **no** form of this command to return to the default settings.

```
radius server name
address {ipv4 | ipv6} ip{address / hostname} auth-port udp-port acct-port udp-port
key string
automate tester name | retransmit value | timeout seconds
no radius server name
```

## Syntax Description

|   |   |
|---|---|
| <b>address</b> { <b>ipv4</b>   <b>ipv6</b> }<br><i>ip{address / hostname}</i> | Specifies the IP address of the RADIUS server.  |
| <b>auth-port</b> <i>udp-port</i>  | (Optional) Specifies the UDP port for the RADIUS authentication server. The range is from 0 to 65536.   |
| <b>acct-port</b> <i>udp-port</i>  | (Optional) Specifies the UDP port for the RADIUS accounting server. The range is from 0 to 65536.   |
| <b>key</b> <i>string</i>  | (Optional) Specifies the authentication and encryption key for all RADIUS communication between the device and the RADIUS daemon.<br><br><b>Note</b> The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in this command. Leading spaces are ignored, but spaces within and at the end of the key are used. If there are spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key. |
| <b>automate tester</b> <i>name</i>  | (Optional) Enables automatic server testing of the RADIUS server status, and specify the username to be used.   |
| <b>retransmit</b> <i>value</i>  | (Optional) Specifies the number of times a RADIUS request is resent when the server is not responding or responding slowly. The range is 1 to 100. This setting overrides the radius-server retransmit global configuration command setting.  |
| <b>timeout</b> <i>seconds</i>   | (Optional) Specifies the time interval that the device waits for the RADIUS server to reply before sending a request again. The range is 1 to 1000. This setting overrides the <b>radius-server timeout</b> command.  |

## Command Default

- The UDP port for the RADIUS accounting server is 1646.
- The UDP port for the RADIUS authentication server is 1645.
- Automatic server testing is disabled.
- The timeout is 60 minutes (1 hour).
- When the automatic testing is enabled, testing occurs on the accounting and authentication UDP ports.



- The authentication and encryption key ( string) is not configured.

### Command Modes

Global configuration (config)

### Command History

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

### Usage Guidelines

- We recommend that you configure the UDP port for the RADIUS accounting server and the UDP port for the RADIUS authentication server to non-default values.
- You can configure the authentication and encryption key by using the **key string** command in RADIUS server configuration mode. Always configure the key as the last item in this command.
- Use the **automate-tester name** keywords to enable automatic server testing of the RADIUS server status and to specify the username to be used.

This example shows how to configure 1645 as the UDP port for the authentication server and 1646 as the UDP port for the accounting server, and configure a key string:

```
Device> enable
Device# configure terminal
Device(config)# radius server ISE
Device(config-radius-server)# address ipv4 10.1.1 auth-port 1645 acct-port 1646
Device(config-radius-server)# key cisco123
Device(config-radius-server)# end
```

# sak-rekey

To configure the Security Association Key (SAK) rekey time interval for a defined MKA policy, use the **sak-rekey** command in MKA-policy configuration mode. To stop the SAK rekey timer, use the **no** form of this command.

**sak-rekey** {**interval** *time-interval* | **on-live-peer-loss**}  
**no sak-rekey** {**interval** | **on-live-peer-loss**}

|                           |                          |  |
|---------------------------|--------------------------|--|
| <b>Syntax Description</b> | <b>interval</b>          | SAK rekey interval in seconds.                       |
|                           | <i>time-interval</i>     | The range is from 30 to 65535, and the default is 0. |
|                           | <b>on-live-peer-loss</b> | Peer loss from the live membership.                  |

**Command Default** The SAK rekey timer is disabled. The default is 0.

**Command Modes** MKA-policy configuration (config-mka-policy)

|                        |                           |                              |
|------------------------|---------------------------|------------------------------|
| <b>Command History</b> | <b>Release</b>            | <b>Modification</b>          |
|                        | Cisco IOS XE Fuji 16.8.1a | This command was introduced. |

## Examples

The following example shows how to configure the SAK rekey interval:

```
Device> enable
Device# configure terminal
Device(config)# mka policy 2
Device(config-mka-policy)# sak-rekey interval 300
```

|                         |                                  |  |
|-------------------------|----------------------------------|--|
| <b>Related Commands</b> | <b>Command</b>                   | <b>Description</b>   |
|                         | <b>mka policy</b>                | Configures an MKA policy.                                      |
|                         | <b>confidentiality-offset</b>    | Sets the confidentiality offset for MACsec operations.         |
|                         | <b>delay-protection</b>          | Configures MKA to use delay protection in sending MKPDU.       |
|                         | <b>include-icv-indicator</b>     | Includes ICV indicator in MKPDU.                               |
|                         | <b>key-server</b>                | Configures MKA key-server options.                             |
|                         | <b>macsec-cipher-suite</b>       | Configures cipher suite for deriving SAK.                      |
|                         | <b>send-secure-announcements</b> | Configures MKA to send secure announcements in sending MKPDUs. |
|                         | <b>ssci-based-on-sci</b>         | Computes SSCI based on the SCI.                                |
|                         | <b>use-updated-eth-header</b>    | Uses the updated Ethernet header for ICV calculation.          |

## 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** }

|                           |  |  |
|---------------------------|--|--|
| <b>Syntax Description</b> | <b>glean</b>                                       | Extracts addresses from the messages and installs them into the binding table without performing any verification.   |
|                           | <b>guard</b>                                       | 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. |
|                           | <b>inspect</b>                                     | Validates messages for consistency and conformance; in particular, address ownership is enforced. Invalid messages are dropped.  |
| <b>Command Default</b>    | The default security level is guard.               |  |
| <b>Command Modes</b>      | IPv6 snooping configuration (config-ipv6-snooping) |  |
| <b>Command History</b>    | <b>Release</b>                                     | <b>Modification</b>  |
|                           | Cisco IOS XE Everest 16.6.1                        | This command was introduced.   |

This example shows how to define an IPv6 snooping policy name as policy1 and configure the security level as inspect:

```
Device> enable
Device# configure terminal
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# security-level inspect
Device(config-ipv6-snooping)# end
```

# send-secure-announcements

To enable MKA to send secure announcements in MACsec Key Agreement Protocol Data Units (MKPDUs), use the **send-secure-announcements** command in MKA-policy configuration mode. To disable sending of secure announcements, use the **no** form of this command.

**send-secure-announcements**  
**no send-secure-announcements**

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

**Command Default** Secure announcements in MKPDUs is disabled.

**Command Modes** MKA-policy configuration (config-mka-policy)

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

**Usage Guidelines** Secure announcements revalidate the MACsec Cipher Suite capabilities which were shared previously through unsecure announcements.

**Examples** The following example shows how to enable sending of secure announcements:

```
Device> enable
Device# configure terminal
Device(config)# mka policy 2
Device(config-mka-policy)# send-secure-announcements
```

| Related Commands | Command                       | Description  |
|------------------|-------------------------------|--|
|                  | <b>mka policy</b>             | Configures an MKA policy.                                |
|                  | <b>confidentiality-offset</b> | Sets the confidentiality offset for MACsec operations.   |
|                  | <b>delay-protection</b>       | Configures MKA to use delay protection in sending MKPDU. |
|                  | <b>include-icv-indicator</b>  | Includes ICV indicator in MKPDU.                         |
|                  | <b>key-server</b>             | Configures MKA key-server options.                       |
|                  | <b>macsec-cipher-suite</b>    | Configures cipher suite for deriving SAK.                |
|                  | <b>sak-rekey</b>              | Configures the SAK rekey interval.                       |
|                  | <b>ssci-based-on-sci</b>      | Computes SSCI based on the SCI.                          |
|                  | <b>use-updated-eth-header</b> | Uses the updated ethernet header for ICV calculation.    |

## server-private (RADIUS)

To configure the IP address of the private RADIUS server for the group server, use the **server-private** command in RADIUS server-group configuration mode. To remove the associated private server from the authentication, authorization, and accounting (AAA) group server, use the **no** form of this command.

**server-private** *ip-address* [{**auth-port** *port-number* | **acct-port** *port-number*}] [**non-standard**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]  
**no server-private** *ip-address* [{**auth-port** *port-number* | **acct-port** *port-number*}] [**non-standard**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]

### Syntax Description

|                                     |   |
|-------------------------------------|---|
| <i>ip-address</i>                   | IP address of the private RADIUS server host.   |
| <b>auth-port</b> <i>port-number</i> | (Optional) User Datagram Protocol (UDP) destination port for authentication requests. The default value is 1645.  |
| <b>acct-port</b> <i>port-number</i> | (Optional) UDP destination port for accounting requests. The default value is 1646.   |
| <b>non-standard</b>                 | (Optional) RADIUS server is using vendor-proprietary RADIUS attributes.   |
| <b>timeout</b> <i>seconds</i>       | (Optional) Time interval (in seconds) that the device waits for the RADIUS server to reply before retransmitting. This setting overrides the global value of the <b>radius-server timeout</b> command. If no timeout value is specified, the global value is used.  |
| <b>retransmit</b> <i>retries</i>    | (Optional) Number of times a RADIUS request is resent to a server, if that server is not responding or responding slowly. This setting overrides the global setting of the <b>radius-server retransmit</b> command.   |
| <b>key</b> <i>string</i>            | (Optional) Authentication and encryption key used between the device and the RADIUS daemon running on the RADIUS server. This key overrides the global setting of the <b>radius-server key</b> command. If no key string is specified, the global value is used.<br><br>The <i>string</i> can be <b>0</b> (specifies that an unencrypted key follows), <b>6</b> (specifies that an advanced encryption scheme [AES] encrypted key follows), <b>7</b> (specifies that a hidden key follows), or a line specifying the unencrypted (clear-text) server key. |

### Command Default

If server-private parameters are not specified, global configurations will be used; if global configurations are not specified, default values will be used.

### Command Modes

RADIUS server-group configuration (config-sg-radius)

### Command History

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

### Usage Guidelines

Use the **server-private** command to associate a particular private server with a defined server group. To prevent possible overlapping of private addresses between virtual route forwarding (VRF) instances, private

servers (servers with private addresses) can be defined within the server group and remain hidden from other groups, while the servers in the global pool (default "radius" server group) can still be referred to by IP addresses and port numbers. Thus, the list of servers in server groups includes references to the hosts in the global configuration and the definitions of private servers.

**Note**

- If the **radius-server directed-request** command is configured, then a private RADIUS server cannot be used as the group server by configuring the **server-private** (RADIUS) command.
- Creating or updating AAA server statistics record for private RADIUS servers are not supported. If private RADIUS servers are used, then error messages and tracebacks will be encountered, but these error messages or tracebacks do not have any impact on the AAA RADIUS functionality. To avoid these error messages and tracebacks, configure public RADIUS server instead of private RADIUS server.

Use the **password encryption aes** command to configure type 6 AES encrypted keys.

**Examples**

The following example shows how to define the sg\_water RADIUS group server and associate private servers with it:

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa group server radius sg_water
Device(config-sg-radius)# server-private 10.1.1.1 timeout 5 retransmit 3 key xyz
Device(config-sg-radius)# server-private 10.2.2.2 timeout 5 retransmit 3 key xyz
Device(config-sg-radius)# end
```

**Related Commands**

| Command                               | Description  |
|---------------------------------------|--|
| <b>aaa group server</b>               | Groups different server hosts into distinct lists and distinct methods.              |
| <b>aaa new-model</b>                  | Enables the AAA access control model.  |
| <b>password encryption aes</b>        | Enables a type 6 encrypted preshared key.  |
| <b>radius-server host</b>             | Specifies a RADIUS server host.  |
| <b>radius-server directed-request</b> | Allows users to log in to a Cisco NAS and select a RADIUS server for authentication. |

## server-private (TACACS+)

To configure the IPv4 or IPv6 address of the private TACACS+ server for the group server, use the **server-private** command in server-group configuration mode. To remove the associated private server from the authentication, authorization, and accounting (AAA) group server, use the **no** form of this command.

```
server-private { ipv4-address | ipv6-address | fqdn } [ nat ] [ single-connection ] [ port port-number ] [ timeout seconds ] key [ { 0 | 7 } ] string
no server-private
```

|                    |  |   |
|--------------------|--|---|
| Syntax Description | <i>ipv4-address</i>  | IPv4 address of the private TACACS+ server host.  |
|                    | <i>ipv6-address</i>  | IPv6 address of the private TACACS+ server host.  |
|                    | <b>fqdn</b>  | Fully qualified domain name (fqdn) of the private TACACS+ server host for address resolution from the Domain Name Server (DNS)  |
|                    | <b>nat</b>   | (Optional) Specifies the port Network Address Translation (NAT) address of the remote device. This address is sent to the TACACS+ server.   |
|                    | <b>single-connection</b>   | (Optional) Maintains a single TCP connection between the router and the TACACS+ server.   |
|                    | <b>timeout</b> <i>seconds</i>  | (Optional) Specifies a timeout value for the server response. This value overrides the global timeout value set with the <b>tacacs-server timeout</b> command for this server only.   |
|                    | <b>port</b> <i>port-number</i>   | (Optional) Specifies a server port number. This option overrides the default, which is port 49.   |
|                    | <b>key</b> [ <b>0</b>   <b>7</b> ] <i>string</i>   | (Optional) Specifies an authentication and encryption key. This key must match the key used by the TACACS+ daemon. Specifying this key overrides the key set by the global <b>tacacs-server key</b> command for this server only.<br><br>If no number or 0 is entered, the <i>string</i> that is entered is considered to be plain text. If 7 is entered, the <i>string</i> that is entered is considered to be encrypted text. |
| Command Default    | If server-private parameters are not specified, global configurations will be used; if global configurations are not specified, default values will be used.   |   |
| Command Modes      | TACACS+ server-group configuration (config-sg-tacacs+)   |   |
| Command History    | Release  | Modification  |
|                    | Cisco IOS XE Everest 16.6.1  | This command was introduced.  |
| Usage Guidelines   | Use the <b>server-private</b> command to associate a particular private server with a defined server group. To prevent possible overlapping of private addresses between virtual route forwardings (VRFs), private servers (servers with private addresses) can be defined within the server group and remain hidden from other groups, while the servers in the global pool (default "TACACS+" server group) can still be referred to by IP addresses |   |

and port numbers. Thus, the list of servers in server groups includes references to the hosts in the global configuration and the definitions of private servers.

The following example shows how to define the tacacs1 TACACS+ group server and associate private servers with it:

```
Device> enable
Device# configure terminal
Device(config)# aaa group server tacacs+ tacacs1
Device(config-sg-tacacs+)# server-private 10.1.1.1 port 19 key cisco
Device(config-sg-tacacs+)# exit
Device(config)# ip vrf cisco
Device(config-vrf)# rd 100:1
Device(config-vrf)# exit
Device(config)# interface Loopback0
Device(config-if)# ip address 10.0.0.2 255.0.0.0
Device(config-if)# ip vrf forwarding cisco
```

#### Related Commands

| Command                                 | Description  |
|---|--|
| <b>aaa group server</b>                 | Groups different server hosts into distinct lists and distinct methods.        |
| <b>aaa new-model</b>                    | Enables the AAA access control model.  |
| <b>ip tacacs source-interface</b>       | Uses the IP address of a specified interface for all outgoing TACACS+ packets. |
| <b>ip vrf forwarding (server-group)</b> | Configures the VRF reference of an AAA TACACS+ server group.                   |



# show aaa clients

To display authentication, authorization, and accounting (AAA) client statistics, use the **show aaa clients** command.

**show aaa clients** [**detailed**]

|                           |  |                              |
|---------------------------|--|------------------------------|
| <b>Syntax Description</b> | <b>detailed</b> (Optional) Shows detailed AAA client statistics. |                              |
| <b>Command Modes</b>      | User EXEC (>)<br>Privileged EXEC (#)                             |                              |
| <b>Command History</b>    | <b>Release</b>   | <b>Modification</b>          |
|                           | Cisco IOS XE Everest 16.6.1                                      | This command was introduced. |

This is an example of output from the **show aaa clients** command:

```
Device> enable
Device# show aaa clients

Dropped request packets: 0
```

# show aaa command handler

To display authentication, authorization, and accounting (AAA) command handler statistics, use the **show aaa command handler** command.

## show aaa command handler

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> | This command has no arguments or keywords. |
|---------------------------|--|

|                      |                                      |
|----------------------|--------------------------------------|
| <b>Command Modes</b> | User EXEC (>)<br>Privileged EXEC (#) |
|----------------------|--------------------------------------|

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

This is an example of output from the **show aaa command handler** command:

```
Device# show aaa command handler

AAA Command Handler Statistics:
  account-logon: 0, account-logout: 0
  account-query: 0, pod: 0
  service-logon: 0, service-logout: 0
  user-profile-push: 0, session-state-log: 0
  reauthenticate: 0, bounce-host-port: 0
  disable-host-port: 0, update-rbac: 0
  update-ssl: 0, update-cts-policies: 0
  invalid commands: 0
  async message not sent: 0
```

# show aaa local

To display authentication, authorization, and accounting (AAA) local method options, use the **show aaa local** command.

**show aaa local** { **netuser** { *name* | **all** } | **statistics** | **user lockout** }

## Syntax Description

|                     |   |
|---------------------|---|
| <b>netuser</b>      | Specifies the AAA local network or guest user database. |
| <i>name</i>         | Network user name.                                      |
| <b>all</b>          | Specifies the network and guest user information.       |
| <b>statistics</b>   | Displays statistics for local authentication.           |
| <b>user lockout</b> | Specifies the AAA local locked-out user.                |

## Command Modes

User EXEC (>)  
Privileged EXEC (#)

## Command History

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

This is an example of output from the **show aaa local statistics** command:

```
Device# show aaa local statistics
```

```
Local EAP statistics
```

| EAP Method   | Success | Fail |
|--------------|---------|------|
| Unknown      | 0       | 0    |
| EAP-MD5      | 0       | 0    |
| EAP-GTC      | 0       | 0    |
| LEAP         | 0       | 0    |
| PEAP         | 0       | 0    |
| EAP-TLS      | 0       | 0    |
| EAP-MSCHAPV2 | 0       | 0    |
| EAP-FAST     | 0       | 0    |

```
Requests received from AAA: 0
Responses returned from EAP: 0
Requests dropped (no EAP AVP): 0
Requests dropped (other reasons): 0
Authentication timeouts from EAP: 0
```

```
Credential request statistics
```

```
Requests sent to backend: 0
Requests failed (unable to send): 0
Authorization results received
```

```
Success: 0
```

 show aaa local

Fail:

0

# show aaa servers

To display all authentication, authorization, and accounting (AAA) servers as seen by the AAA server MIB, use the **show aaa servers** command.

**show aaa servers** [**private** | **public** | [**detailed**]]

|                           |                             |  |
|---------------------------|-----------------------------|--|
| <b>Syntax Description</b> | <b>detailed</b>             | (Optional) Displays private AAA servers as seen by the AAA server MIB. |
|                           | <b>public</b>               | (Optional) Displays public AAA servers as seen by the AAA server MIB.  |
|                           | <b>detailed</b>             | (Optional) Displays detailed AAA server statistics.                    |
| <b>Command Modes</b>      | User EXEC (>)               |  |
|                           | Privileged EXEC (>)         |  |
| <b>Command History</b>    | <b>Release</b>              | <b>Modification</b>  |
|                           | Cisco IOS XE Everest 16.6.1 | This command was introduced.   |

## Examples

The following is a sample output from the **show aaa servers** command:

```
Device# show aaa servers

RADIUS: id 1, priority 1, host 172.20.128.2, auth-port 1645, acct-port 1646
State: current UP, duration 9s, previous duration 0s
Dead: total time 0s, count 0
Quarantined: No
Authen: request 0, timeouts 0, failover 0, retransmission 0
Response: accept 0, reject 0, challenge 0
Response: unexpected 0, server error 0, incorrect 0, time 0ms
Transaction: success 0, failure 0
Throttled: transaction 0, timeout 0, failure 0
Author: request 0, timeouts 0, failover 0, retransmission 0
Response: accept 0, reject 0, challenge 0
Response: unexpected 0, server error 0, incorrect 0, time 0ms
Transaction: success 0, failure 0
Throttled: transaction 0, timeout 0, failure 0
Account: request 0, timeouts 0, failover 0, retransmission 0
Request: start 0, interim 0, stop 0
Response: start 0, interim 0, stop 0
Response: unexpected 0, server error 0, incorrect 0, time 0ms
Transaction: success 0, failure 0
Throttled: transaction 0, timeout 0, failure 0
Elapsed time since counters last cleared: 0m
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
```

# show aaa sessions

To display authentication, authorization, and accounting (AAA) sessions as seen by the AAA Session MIB, use the **show aaa sessions** command.

## show aaa sessions

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> | This command has no arguments or keywords. |
|---------------------------|--|

|                      |                                      |
|----------------------|--------------------------------------|
| <b>Command Modes</b> | User EXEC (>)<br>Privileged EXEC (#) |
|----------------------|--------------------------------------|

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

The following is sample output from the **show aaa sessions** command:

```
Device# show aaa sessions

Total sessions since last reload: 7
Session Id: 4007
  Unique Id: 4025
  User Name: *not available*
  IP Address: 0.0.0.0
  Idle Time: 0
  CT Call Handle: 0
```

# show authentication brief

To display brief information about authentication sessions for a given interface, use the **show authentication brief** command in either user EXEC or privileged EXEC mode.

```
show authentication brief [switch {switch-number | active | standby} {R0}]
```

|                           |                             |   |
|---------------------------|-----------------------------|---|
| <b>Syntax Description</b> | <i>switch-number</i>        | Valid values for the <i>switch-number</i> variable are from 1 to 9. |
|                           | <b>R0</b>                   | Displays information about the Route Processor (RP) slot 0.         |
|                           | <b>active</b>               | Specifies the active instance.                                      |
|                           | <b>standby</b>              | Specifies the standby instance.                                     |
| <b>Command Modes</b>      | Privileged EXEC (#)         |   |
|                           | User EXEC (>)               |   |
| <b>Command History</b>    | <b>Release</b>              | <b>Modification</b>   |
|                           | Cisco IOS XE Everest 16.6.1 | This command was introduced.  |

The following is a sample output from the **show authentication brief** command:

```
Device# show authentication brief
```

| Interface | MAC Address    | AuthC     | AuthZ   | Eg | Uptime |
|-----------|----------------|-----------|---------|----|--------|
| Gi2/0/14  | 0002.0002.0001 | m:NA d:OK | AZ: SA- | X  | 281s   |
| Gi2/0/14  | 0002.0002.0002 | m:NA d:OK | AZ: SA- | X  | 280s   |
| Gi2/0/14  | 0002.0002.0003 | m:NA d:OK | AZ: SA- | X  | 279s   |
| Gi2/0/14  | 0002.0002.0004 | m:NA d:OK | AZ: SA- | X  | 278s   |
| Gi2/0/14  | 0002.0002.0005 | m:NA d:OK | AZ: SA- | X  | 278s   |
| Gi2/0/14  | 0002.0002.0006 | m:NA d:OK | AZ: SA- | X  | 277s   |
| Gi2/0/14  | 0002.0002.0007 | m:NA d:OK | AZ: SA- | X  | 276s   |
| Gi2/0/14  | 0002.0002.0008 | m:NA d:OK | AZ: SA- | X  | 276s   |
| Gi2/0/14  | 0002.0002.0009 | m:NA d:OK | AZ: SA- | X  | 275s   |
| Gi2/0/14  | 0002.0002.000a | m:NA d:OK | AZ: SA- | X  | 275s   |
| Gi2/0/14  | 0002.0002.000b | m:NA d:OK | AZ: SA- | X  | 274s   |
| Gi2/0/14  | 0002.0002.000c | m:NA d:OK | AZ: SA- | X  | 274s   |
| Gi2/0/14  | 0002.0002.000d | m:NA d:OK | AZ: SA- | X  | 273s   |
| Gi2/0/14  | 0002.0002.000e | m:NA d:OK | AZ: SA- | X  | 273s   |
| Gi2/0/14  | 0002.0002.000f | m:NA d:OK | AZ: SA- | X  | 272s   |
| Gi2/0/14  | 0002.0002.0010 | m:NA d:OK | AZ: SA- | X  | 272s   |
| Gi2/0/14  | 0002.0002.0011 | m:NA d:OK | AZ: SA- | X  | 271s   |
| Gi2/0/14  | 0002.0002.0012 | m:NA d:OK | AZ: SA- | X  | 271s   |
| Gi2/0/14  | 0002.0002.0013 | m:NA d:OK | AZ: SA- | X  | 270s   |
| Gi2/0/14  | 0002.0002.0014 | m:NA d:OK | AZ: SA- | X  | 270s   |
| Gi2/0/14  | 0002.0002.0015 | m:NA d:OK | AZ: SA- | X  | 269s   |

The following is a sample output from the **show authentication brief** command for active instances:

Device# **show authentication brief switch active R0**

| Interface | MAC Address    | AuthC     | AuthZ   | Fg | Uptime |
|-----------|----------------|-----------|---------|----|--------|
| Gi2/0/14  | 0002.0002.0001 | m:NA d:OK | AZ: SA- | X  | 1s     |
| Gi2/0/14  | 0002.0002.0002 | m:NA d:OK | AZ: SA- | X  | 0s     |
| Gi2/0/14  | 0002.0002.0003 | m:NA d:OK | AZ: SA- | X  | 299s   |
| Gi2/0/14  | 0002.0002.0004 | m:NA d:OK | AZ: SA- | X  | 298s   |
| Gi2/0/14  | 0002.0002.0005 | m:NA d:OK | AZ: SA- | X  | 298s   |
| Gi2/0/14  | 0002.0002.0006 | m:NA d:OK | AZ: SA- | X  | 297s   |
| Gi2/0/14  | 0002.0002.0007 | m:NA d:OK | AZ: SA- | X  | 296s   |
| Gi2/0/14  | 0002.0002.0008 | m:NA d:OK | AZ: SA- | X  | 296s   |
| Gi2/0/14  | 0002.0002.0009 | m:NA d:OK | AZ: SA- | X  | 295s   |
| Gi2/0/14  | 0002.0002.000a | m:NA d:OK | AZ: SA- | X  | 295s   |
| Gi2/0/14  | 0002.0002.000b | m:NA d:OK | AZ: SA- | X  | 294s   |
| Gi2/0/14  | 0002.0002.000c | m:NA d:OK | AZ: SA- | X  | 294s   |
| Gi2/0/14  | 0002.0002.000d | m:NA d:OK | AZ: SA- | X  | 293s   |
| Gi2/0/14  | 0002.0002.000e | m:NA d:OK | AZ: SA- | X  | 293s   |
| Gi2/0/14  | 0002.0002.000f | m:NA d:OK | AZ: SA- | X  | 292s   |
| Gi2/0/14  | 0002.0002.0010 | m:NA d:OK | AZ: SA- | X  | 292s   |
| Gi2/0/14  | 0002.0002.0011 | m:NA d:OK | AZ: SA- | X  | 291s   |
| Gi2/0/14  | 0002.0002.0012 | m:NA d:OK | AZ: SA- | X  | 291s   |
| Gi2/0/14  | 0002.0002.0013 | m:NA d:OK | AZ: SA- | X  | 290s   |
| Gi2/0/14  | 0002.0002.0014 | m:NA d:OK | AZ: SA- | X  | 290s   |
| Gi2/0/14  | 0002.0002.0015 | m:NA d:OK | AZ: SA- | X  | 289s   |
| Gi2/0/14  | 0002.0002.0016 | m:NA d:OK | AZ: SA- | X  | 289s   |

The following is a sample output from the **show authentication brief** command for standby instances:

Device# **show authentication brief switch standby R0**

No sessions currently exist

The table below describes the significant fields shown in the displays.

**Table 4: show authentication brief Field Descriptions**

| Field       | Description  |
|-------------|--|
| Interface   | The type and number of the authentication interface. |
| MAC Address | The MAC address of the client.                       |
| AuthC       | Indicates authentication status.                     |
| AuthZ       | Indicates authorization status.                      |



| Field  | Description   |
|--------|---|
| Fg     | Flag indicates the current status. The valid values are: <ul style="list-style-type: none"><li>• A—Applying policy (multi-line status for details)</li><li>• D—Awaiting removal</li><li>• F—Final removal in progress</li><li>• I—Awaiting IIF ID allocation</li><li>• P—Pushed session</li><li>• R—Removing user profile (multi-line status for details)</li><li>• U—Applying user profile (multi-line status for details)</li><li>• X—Unknown blocker</li></ul> |
| Uptime | Indicates the duration since which the session came up  |

# show authentication sessions

To display information about current Auth Manager sessions, use the **show authentication sessions** command.

**show authentication sessions** [**database**] [**handle** *handle-id* [**details**]] [**interface** *type number* [**details**]] [**mac** *mac-address* [**interface** *type number*]] [**method** *method-name* [**interface** *type number* [**details**]]] [**session-id** *session-id* [**details**]]

## Syntax Description

|                                     |  |
|-------------------------------------|--|
| <b>database</b>                     | (Optional) Shows only data stored in session database.   |
| <b>handle</b> <i>handle-id</i>      | (Optional) Specifies the particular handle for which Auth Manager information is to be displayed.  |
| <b>details</b>                      | (Optional) Shows detailed information.   |
| <b>interface</b> <i>type number</i> | (Optional) Specifies a particular interface type and number for which Auth Manager information is to be displayed.   |
| <b>mac</b> <i>mac-address</i>       | (Optional) Specifies the particular MAC address for which you want to display information.   |
| <b>method</b> <i>method-name</i>    | (Optional) Specifies the particular authentication method for which Auth Manager information is to be displayed. If you specify a method ( <b>dot1x</b> , <b>mab</b> , or <b>webauth</b> ), you may also specify an interface. |
| <b>session-id</b> <i>session-id</i> | (Optional) Specifies the particular session for which Auth Manager information is to be displayed.   |

## Command Modes

User EXEC (>)

Privileged EXEC (#)

## Command History

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

## Usage Guidelines

Use the **show authentication sessions** command to display information about all current Auth Manager sessions. To display information about specific Auth Manager sessions, use one or more of the keywords.

This table shows the possible operating states for the reported authentication sessions.

**Table 5: Authentication Method States**

| State       | Description  |
|-------------|--|
| Not run     | The method has not run for this session.                                   |
| Running     | The method is running for this session.                                    |
| Failed over | The method has failed and the next method is expected to provide a result. |

| State        | Description   |
|--------------|---|
| Success      | The method has provided a successful authentication result for the session. |
| Authc Failed | The method has provided a failed authentication result for the session.     |

This table shows the possible authentication methods.

**Table 6: Authentication Method States**

| State   | Description               |
|---------|---------------------------|
| dot1x   | 802.1X                    |
| mab     | MAC authentication bypass |
| webauth | web authentication        |

The following example shows how to display all authentication sessions on the device:

```
Device# show authentication sessions
```

```
Interface    MAC Address    Method    Domain    Status    Session ID
Gil/0/48     0015.63b0.f676 dot1x     DATA     Authz Success 0A3462B10000000102983C05C
Gil/0/5      000f.23c4.a401 mab       DATA     Authz Success 0A3462B10000000D24F80B58
Gil/0/5      0014.bf5d.d26d dot1x     DATA     Authz Success 0A3462B10000000E29811B94
```

The following example shows how to display all authentication sessions on an interface:

```
Device# show authentication sessions interface gigabitethernet2/0/47
```

```

      Interface: GigabitEthernet2/0/47
      MAC Address: Unknown
      IP Address: Unknown
      Status: Authz Success
      Domain: DATA
      Oper host mode: multi-host
      Oper control dir: both
      Authorized By: Guest Vlan
      Vlan Policy: 20
      Session timeout: N/A
      Idle timeout: N/A
      Common Session ID: 0A3462C800000000000002763C
      Acct Session ID: 0x00000002
      Handle: 0x25000000
Runnable methods list:
  Method    State
  mab       Failed over
  dot1x     Failed over
-----
      Interface: GigabitEthernet2/0/47
      MAC Address: 0005.5e7c.da05
      IP Address: Unknown
      User-Name: 00055e7cda05
      Status: Authz Success
```

## ■ show authentication sessions

```
Domain: VOICE
Oper host mode: multi-domain
Oper control dir: both
Authorized By: Authentication Server
Session timeout: N/A
Idle timeout: N/A
Common Session ID: 0A3462C8000000010002A238
Acct Session ID: 0x00000003
Handle: 0x91000001
Runnable methods list:
Method    State
mab       Authc Success
dot1x     Not run
```

# show cisp

To display Client Information Signaling Protocol (CISP) information for a specified interface, use the **show cisp** command in privileged EXEC mode.

**show cisp** { [**clients** | **interface** *interface-id*] | **registrations** | **summary** }

| Syntax Description | <b>clients</b>                       | (Optional) Display CISP client details.                                     |
|--------------------|--------------------------------------|---|
|                    | <b>interface</b> <i>interface-id</i> | (Optional) Display CISP information about the specified interface channels. |
|                    | <b>registrations</b>                 | Displays CISP registrations.  |
|                    | <b>summary</b>                       | (Optional) Displays CISP summary.   |
| Command Modes      | Privileged EXEC (#)                  |   |
| Command History    | Release                              | Modification  |
|                    | Cisco IOS XE Everest 16.6.1          | This command was introduced.  |

The following is sample output from the **show cisp interface** command:

```
Device# show cisp interface fastethernet 0/1/1

CISP not enabled on specified interface
```

The following is sample output from the **show cisp registration** command:

```
Device# show cisp registrations

Interface(s) with CISP registered user(s):
-----
Fa1/0/13
Auth Mgr (Authenticator)
Gi2/0/1
Auth Mgr (Authenticator)
Gi2/0/2
Auth Mgr (Authenticator)
Gi2/0/3
Auth Mgr (Authenticator)
Gi2/0/5
Auth Mgr (Authenticator)
Gi2/0/9
Auth Mgr (Authenticator)
Gi2/0/11
Auth Mgr (Authenticator)
Gi2/0/13
Auth Mgr (Authenticator)
Gi3/0/3
Gi3/0/5
```

Gi3/0/23

**Related Commands**

| Command                                 | Description                                  |
|---|--|
| <b>cisp enable</b>                      | Enables CISP.                                |
| <b>dot1x credentials</b> <i>profile</i> | Configures a profile on a supplicant device. |

# show dot1x

To display IEEE 802.1x statistics, administrative status, and operational status for a device or for the specified port, use the **show dot1x** command in user EXEC or privileged EXEC mode.

**show dot1x** [**all** [**count** | **details** | **statistics** | **summary**]] [**interface** *type number* [**details** | **statistics**]] [**statistics**]

| Syntax Description                  |  |  |
|-------------------------------------|--|--|
| <b>all</b>                          |  | (Optional) Displays the IEEE 802.1x information for all interfaces.      |
| <b>count</b>                        |  | (Optional) Displays total number of authorized and unauthorized clients. |
| <b>details</b>                      |  | (Optional) Displays the IEEE 802.1x interface details.                   |
| <b>statistics</b>                   |  | (Optional) Displays the IEEE 802.1x statistics for all interfaces.       |
| <b>summary</b>                      |  | (Optional) Displays the IEEE 802.1x summary for all interfaces.          |
| <b>interface</b> <i>type number</i> |  | (Optional) Displays the IEEE 802.1x status for the specified port.       |

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

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

The following is sample output from the **show dot1x all** command:

```
Device# show dot1x all

Sysauthcontrol           Enabled
Dot1x Protocol Version   3
```

The following is sample output from the **show dot1x all count** command:

```
Device# show dot1x all count

Number of Dot1x sessions
-----
Authorized Clients       = 0
Unauthorized Clients     = 0
Total No of Client       = 0
```

The following is sample output from the **show dot1x all statistics** command:

```
Device# show dot1x statistics
```

Dot1x Global Statistics for

```
-----  
RxStart = 0      RxLogoff = 0      RxResp = 0      RxRespID = 0  
RxReq = 0        RxInvalid = 0     RxLenErr = 0  
RxTotal = 0  
  
TxStart = 0      TxLogoff = 0      TxResp = 0  
TxReq = 0        ReTxReq = 0       ReTxReqFail = 0  
TxReqID = 0      ReTxReqID = 0     ReTxReqIDFail = 0  
TxTotal = 0
```



## show eap pac peer

To display stored Protected Access Credentials (PAC) for Extensible Authentication Protocol (EAP) Flexible Authentication via Secure Tunneling (FAST) peers, use the **show eap pac peer** command in privileged EXEC mode.

### show eap pac peer

#### Syntax Description

This command has no arguments or keywords.

#### Command Modes

Privileged EXEC (#)

#### Command History

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

The following is sample output from the **show eap pac peers** command:

```
Device# show eap pac peers
No PACs stored
```

#### Related Commands

| Command                   | Description  |
|---------------------------|--|
| <b>clear eap sessions</b> | Clears EAP session information for the device or for the |

# show ip access-lists

To display the contents of all current IP access lists, use the **show ip access-lists** command in user EXEC or privileged EXEC modes.

**show ip access-lists** [{ *access-list-number* *access-list-number-expanded-range* *access-list-name* | **dynamic** [*dynamic-access-list-name*] | **interface** *name* *number* [{ **in** | **out** }]}]

## Syntax Description

|  |  |
|--|--|
| <i>access-list-number</i>                      | (Optional) Number of the IP access list to display.              |
| <i>access-list-number-expanded-range</i>       | (Optional) Expanded range of the IP access list to display.      |
| <i>access-list-name</i>                        | (Optional) Name of the IP access list to display.                |
| <b>dynamic</b> <i>dynamic-access-list-name</i> | (Optional) Displays the specified dynamic IP access lists.       |
| <b>interface</b> <i>name</i> <i>number</i>     | (Optional) Displays the access list for the specified interface. |
| <b>in</b>                                      | (Optional) Displays input interface statistics.                  |
| <b>out</b>                                     | (Optional) Displays output interface statistics.                 |



**Note** Statistics for OGACL is not supported

## Command Default

All standard and expanded IP access lists are displayed.

## Command Modes

User EXEC (>)

Privileged EXEC (#)

## Command History

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

## Usage Guidelines

The **show ip access-lists** command provides output identical to the **show access-lists** command, except that it is IP-specific and allows you to specify a particular access list.

The output of the **show ip access-lists interface** command does not display dACL or ACL filter IDs. This is because the ACLs are attached to the virtual ports created by multidomain authentication for each authentication session; instead of the physical interface. To display dACL or ACL filter IDs, use the **show ip access-lists access-list-name** command. The *access-list-name* should be taken from the **show access-session interface interface-name detail** command output. The *access-list-name* is case sensitive.

## Examples

The following is a sample output from the **show ip access-lists** command when all access lists are requested:

```
Device# show ip access-lists

Extended IP access list 101
  deny udp any any eq nntp
  permit tcp any any
  permit udp any any eq tftp
  permit icmp any any
  permit udp any any eq domain
```

The table below describes the significant fields shown in the display.

**Table 7: show ip access-lists Field Descriptions**

| Field                   | Description                          |
|-------------------------|--------------------------------------|
| Extended IP access list | Extended IP access-list name/number. |
| deny                    | Packets to reject.                   |
| udp                     | User Datagram Protocol.              |
| any                     | Source host or destination host.     |
| eq                      | Packets on a given port number.      |
| nntp                    | Network News Transport Protocol.     |
| permit                  | Packets to forward.                  |
| tcp                     | Transmission Control Protocol.       |
| tftp                    | Trivial File Transfer Protocol.      |
| icmp                    | Internet Control Message Protocol.   |
| domain                  | Domain name service.                 |

The following is a sample output from the **show ip access-lists** command when the name of a specific access list is requested:

```
Device# show ip access-lists Internetfilter

Extended IP access list Internetfilter
  permit tcp any 192.0.2.0 255.255.255.255 eq telnet
  deny tcp any any
  deny udp any 192.0.2.0 255.255.255.255 lt 1024
  deny ip any any log
```

The following is a sample output from the **show ip access-lists** command using the **dynamic** keyword:

```
Device# show ip access-lists dynamic CM_SF#1

Extended IP access list CM_SF#1
  10 permit udp any any eq 5060 (650 matches)
  20 permit tcp any any eq 5060
  30 permit udp any any dscp ef (806184 matches)
```

**Related Commands**

| Command                          | Description  |
|----------------------------------|--|
| <b>deny</b>                      | Sets conditions in a named IP access list or OGACL that will deny packets.   |
| <b>ip access-group</b>           | Applies an ACL or OGACL to an interface or a service policy map.             |
| <b>ip access-list</b>            | Defines an IP access list or OGACL by name or number.                        |
| <b>object-group network</b>      | Defines network object groups for use in OGACLs.                             |
| <b>object-group service</b>      | Defines service object groups for use in OGACLs.                             |
| <b>permit</b>                    | Sets conditions in a named IP access list or OGACL that will permit packets. |
| <b>show object-group</b>         | Displays information about object groups that are configured.                |
| <b>show run interfaces cable</b> | Displays statistics on the cable modem.                                      |

# show ip dhcp snooping statistics

To display DHCP snooping statistics in summary or detail form, use the **show ip dhcp snooping statistics** command in user EXEC or privileged EXEC mode.

**show ip dhcp snooping statistics** [**detail** ]

|                           |   |                              |
|---------------------------|---|------------------------------|
| <b>Syntax Description</b> | <b>detail</b> (Optional) Displays detailed statistics information.  |                              |
| <b>Command Modes</b>      | User EXEC (>)<br>Privileged EXEC (#)  |                              |
| <b>Command History</b>    | <b>Release</b>  | <b>Modification</b>          |
|                           | Cisco IOS XE Everest 16.6.1   | This command was introduced. |
| <b>Usage Guidelines</b>   | In a device stack, all statistics are generated on the stack's active switch. If a new active device is elected, the statistics counters reset. |                              |

The following is sample output from the **show ip dhcp snooping statistics** command:

```
Device> show ip dhcp snooping statistics
```

```
Packets Forwarded                = 0
Packets Dropped                  = 0
Packets Dropped From untrusted ports = 0
```

The following is sample output from the **show ip dhcp snooping statistics detail** command:

```
Device> show ip dhcp snooping statistics detail
```

```
Packets Processed by DHCP Snooping      = 0
Packets Dropped Because
  IDB not known                         = 0
  Queue full                           = 0
  Interface is in errdisabled           = 0
  Rate limit exceeded                   = 0
  Received on untrusted ports           = 0
  Nonzero giaddr                       = 0
  Source mac not equal to chaddr        = 0
  Binding mismatch                      = 0
  Insertion of opt82 fail               = 0
  Interface Down                       = 0
  Unknown output interface              = 0
  Reply output port equal to input port = 0
  Packet denied by platform            = 0
```

This table shows the DHCP snooping statistics and their descriptions:

**Table 8: DHCP Snooping Statistics**

| DHCP Snooping Statistic               | Description  |
|---------------------------------------|--|
| Packets Processed by DHCP Snooping    | Total number of packets handled by DHCP snooping, including forwarded and dropped packets.   |
| Packets Dropped Because IDB not known | Number of errors when the input interface of the packet cannot be determined.  |
| Queue full                            | Number of errors when an internal queue used to process the packets is full. This might happen if DHCP packets are received at an excessively high rate and rate limiting is not enabled on the ingress ports.   |
| Interface is in errdisabled           | Number of times a packet was received on a port that has been marked as error disabled. This might happen if packets are in the processing queue when a port is put into the error-disabled state and those packets are subsequently processed.  |
| Rate limit exceeded                   | Number of times the rate limit configured on the port was exceeded and the interface was put into the error-disabled state.  |
| Received on untrusted ports           | Number of times a DHCP server packet (OFFER, ACK, NAK, or LEASEQUERY) was received on an untrusted port and was dropped.   |
| Nonzero giaddr                        | Number of times the relay agent address field (giaddr) in the DHCP packet received on an untrusted port was not zero, or the <b>no ip dhcp snooping information option allow-untrusted</b> global configuration command is not configured and a packet received on an untrusted port contained option-82 data.   |
| Source mac not equal to chaddr        | Number of times the client MAC address field of the DHCP packet (chaddr) does not match the packet source MAC address and the <b>ip dhcp snooping verify mac-address</b> global configuration command is configured.   |
| Binding mismatch                      | Number of times a RELEASE or DECLINE packet was received on a port that is different than the port in the binding for that MAC address-VLAN pair. This indicates someone might be trying to spoof the real client, or it could mean that the client has moved to another port on the device and issued a RELEASE or DECLINE. The MAC address is taken from the chaddr field of the DHCP packet, not the source MAC address in the Ethernet header. |
| Insertion of opt82 fail               | Number of times the option-82 insertion into a packet failed. The insertion might fail if the packet with the option-82 data exceeds the size of a single physical packet on the internet.   |

| DHCP Snooping Statistic               | Description   |
|---------------------------------------|---|
| Interface Down                        | Number of times the packet is a reply to the DHCP relay agent, but the SVI interface for the relay agent is down. This is an unlikely error that occurs if the SVI goes down between sending the client request to the DHCP server and receiving the response.  |
| Unknown output interface              | Number of times the output interface for a DHCP reply packet cannot be determined by either option-82 data or a lookup in the MAC address table. The packet is dropped. This can happen if option 82 is not used and the client MAC address has aged out. If IPSG is enabled with the port-security option and option 82 is not enabled, the MAC address of the client is not learned, and the reply packets will be dropped. |
| Reply output port equal to input port | Number of times the output port for a DHCP reply packet is the same as the input port, causing a possible loop. Indicates a possible network misconfiguration or misuse of trust settings on ports.   |
| Packet denied by platform             | Number of times the packet has been denied by a platform-specific registry.   |

# show radius server-group

To display properties for the RADIUS server group, use the **show radius server-group** command in user EXEC or privileged EXEC mode.

**show radius server-group** {*name* | **all**}

|                           |  |  |
|---------------------------|--|--|
| <b>Syntax Description</b> | <b>name</b>  | Name of the server group. The character string used to name the group of servers must be defined using the <b>aaa group server radius</b> command. |
|                           | <b>all</b>   | Displays properties for all of the server groups.  |
| <b>Command Modes</b>      | User EXEC (>)  |  |
|                           | Privileged EXEC (#)  |  |
| <b>Command History</b>    | <b>Release</b>   | <b>Modification</b>  |
|                           | Cisco IOS XE Everest 16.6.1  | This command was introduced.   |
| <b>Usage Guidelines</b>   | Use the <b>show radius server-group</b> command to display the server groups that you defined by using the <b>aaa group server radius</b> command. |  |
|                           | The following is sample output from the <b>show radius server-group all</b> command:   |  |

```
Device# show radius server-group all

Server group radius
  Sharecount = 1   sg_unconfigured = FALSE
  Type = standard  Memlocks = 1
```

This table describes the significant fields shown in the display.

**Table 9: show radius server-group command Field Descriptions**

| Field           | Description   |
|-----------------|---|
| Server group    | Name of the server group.   |
| Sharecount      | Number of method lists that are sharing this server group. For example, if one method list uses a particular server group, the sharecount would be 1. If two method lists use the same server group, the sharecount would be 2. |
| sg_unconfigured | Server group has been unconfigured.   |



| Field    | Description   |
|----------|---|
| Type     | The type can be either standard or nonstandard. The type indicates whether the servers in the group accept nonstandard attributes. If all servers within the group are configured with the nonstandard option, the type will be shown as "nonstandard".               |
| Memlocks | An internal reference count for the server-group structure that is in memory. The number represents how many internal data structure packets or transactions are holding references to this server group. Memlocks is used internally for memory management purposes. |

# show tech-support acl

To display access control list (ACL)-related information for technical support, use the **show tech-support acl** command in privileged EXEC mode.

## show tech-support acl

### Syntax Description

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. |
| Cisco IOS XE Gibraltar 16.11.1 |                              |

### Usage Guidelines

The output of the **show tech-support acl** command is very long. To better manage this output, you can redirect the output to an external file (for example, **show tech-support acl | redirect flash:show\_tech\_acl.txt**) in the local writable storage file system or remote file system.

The output of this command displays the following commands:



#### Note

On stackable platforms, these commands are executed on every switch in the stack. On modular platforms, like Catalyst 9400 Series Switches, these commands are run only on the active switch.



#### Note

The following list of commands is a sample of the commands available in the output; these may differ based on the platform.

- **show clock**
- **show version**
- **show running-config**
- **show module**
- **show interface**
- **show access-lists**
- **show logging**
- **show platform software fed switch *switch-number* acl counters hardware**
- **show platform software fed switch *switch-number* ifm mapping**
- **show platform hardware fed switch *switch-number* fwd-asic drops exceptions**
- **show platform software fed switch *switch-number* acl info**

- **show platform software fed switch *switch-number* acl**
- **show platform software fed switch *switch-number* acl usage**
- **show platform software fed switch *switch-number* acl policy intftype all cam**
- **show platform software fed switch *switch-number* acl cam brief**
- **show platform software fed switch *switch-number* acl policy intftype all vcu**
- **show platform hardware fed switch *switch-number* acl resource usage**
- **show platform hardware fed switch *switch-number* fwd-asic resource tcam table acl**
- **show platform hardware fed switch *switch-number* fwd-asic resource tcam utilization**
- **show platform software fed switch *switch-number* acl counters hardware**
- **show platform software classification switch *switch-number* all F0 class-group-manager class-group**
- **show platform software process database forwarding-manager switch *switch-number* R0 summary**
- **show platform software process database forwarding-manager switch *switch-number* F0 summary**
- **show platform software object-manager switch *switch-number* F0 pending-ack-update**
- **show platform software object-manager switch *switch-number* F0 pending-issue-update**
- **show platform software object-manager switch *switch-number* F0 error-object**
- **show platform software peer forwarding-manager switch *switch-number* F0**
- **show platform software access-list switch *switch-number* f0 statistics**
- **show platform software access-list switch *switch-number* r0 statistics**
- **show platform software trace message fed switch *switch-number***
- **show platform software trace message forwarding-manager switch *switch-number* F0**
- **show platform software trace message forwarding-manager switch R0 *switch-number* R0**

## Examples

The following is sample output from the **show tech-support acl** command:

```
Device# show tech-support acl
```

```
.
.
.
```

```
----- show platform software fed switch 1 acl cam brief -----
```

```
Printing entries for region ACL_CONTROL (143) type 6 asic 0
```

```
=====
```

```
TAQ-4 Index-0 (A:0,C:0) Valid StartF-1 StartA-1 SkipF-0 SkipA-0
```

```
Output IPv4 VACL
```

```
VCU Result: Not In-Use
```

```
L3 Length: 0000, L3 Protocol: 17 (UDP), L3 Tos: 00
```

```
Source Address/Mask
```

```
0.0.0.0/0.0.0.0
```

Destination Address/Mask  
0.0.0.0/0.0.0.0

Router MAC: Disabled, Not First Fragment: Disabled, Small Offset: Disabled

L4 Source Port/Mask    L4 Destination Port/Mask  
0x0044 (68)/0xffff    0x0043 (67)/0xffff

TCP Flags: 0x00 ( NOT SET )

ACTIONS: Forward L3, Forward L2, Logging Disabled  
ACL Priority: 2 (15 is Highest Priority)

-----  
TAQ-4 Index-1 (A:0,C:0) Valid StartF-0 StartA-0 SkipF-0 SkipA-0  
Output IPv4 VACL

VCU Result: Not In-Use

L3 Length: 0000, L3 Protocol: 17 (UDP), L3 Tos: 00

Source Address/Mask  
0.0.0.0/0.0.0.0  
Destination Address/Mask  
0.0.0.0/0.0.0.0

Router MAC: Disabled, Not First Fragment: Disabled, Small Offset: Disabled

L4 Source Port/Mask    L4 Destination Port/Mask  
0x0043 (67)/0xffff    0x0044 (68)/0xffff

TCP Flags: 0x00 ( NOT SET )

ACTIONS: Forward L3, Forward L2, Logging Disabled  
ACL Priority: 2 (15 is Highest Priority)

-----  
TAQ-4 Index-2 (A:0,C:0) Valid StartF-0 StartA-0 SkipF-0 SkipA-0  
Output IPv4 VACL

VCU Result: Not In-Use

L3 Length: 0000, L3 Protocol: 17 (UDP), L3 Tos: 00

Source Address/Mask  
0.0.0.0/0.0.0.0  
Destination Address/Mask  
0.0.0.0/0.0.0.0

Router MAC: Disabled, Not First Fragment: Disabled, Small Offset: Disabled

L4 Source Port/Mask    L4 Destination Port/Mask  
0x0043 (67)/0xffff    0x0043 (67)/0xffff

TCP Flags: 0x00 ( NOT SET )

ACTIONS: Forward L3, Forward L2, Logging Disabled  
ACL Priority: 2 (15 is Highest Priority)

-----  
TAQ-4 Index-3 (A:0,C:0) Valid StartF-0 StartA-0 SkipF-0 SkipA-0  
Input IPv4 PACL

VCU Result: Not In-Use

```

L3 Length: 0000, L3 Protocol: 00 (HOPOPT), L3 Tos: 00

Source Address/Mask
0.0.0.0/0.0.0.0
Destination Address/Mask
0.0.0.0/0.0.0.0

Router MAC: Disabled, Not First Fragment: Disabled, Small Offset: Disabled

L4 Source Port/Mask    L4 Destination Port/Mask
0x0000 (0)/0x0000      0x0000 (0)/0x0000

TCP Flags: 0x00 ( NOT SET )

ACTIONS:  Drop L3, Drop L2, Logging Disabled
ACL Priority: 2 (15 is Highest Priority)

```

```

-----
TAQ-4 Index-4 (A:0,C:0) Valid StartF-0 StartA-0 SkipF-0 SkipA-0
Output IPv4 PACL

```

```

VCU Result: Not In-Use

L3 Length: 0000, L3 Protocol: 00 (HOPOPT), L3 Tos: 00

Source Address/Mask
0.0.0.0/0.0.0.0
Destination Address/Mask
0.0.0.0/0.0.0.0

Router MAC: Disabled, Not First Fragment: Disabled, Small Offset: Disabled

L4 Source Port/Mask    L4 Destination Port/Mask
0x0000 (0)/0x0000      0x0000 (0)/0x0000

TCP Flags: 0x00 ( NOT SET )

ACTIONS:  Drop L3, Drop L2, Logging Disabled
ACL Priority: 2 (15 is Highest Priority)

```

```

-----
TAQ-4 Index-5 (A:0,C:0) Valid StartF-0 StartA-0 SkipF-0 SkipA-0
Output MAC PACL

```

```

VLAN ID/MASK : 0x000 (000)/0x000

Source MAC/Mask : 0000.0000.0000/0000.0000.0000

Destination MAC/Mask : 0000.0000.0000/0000.0000.0000

isSnap: Disabled, isLLC: Disabled

ACTIONS:  Drop L3, Drop L2, Logging Disabled
ACL Priority: 2 (15 is Highest Priority)

```

```

.
.
.

```

Output fields are self-explanatory.

# show tech-support identity

To display identity/802.1x-related information for technical support, use the **show tech-support identity** command in privileged EXEC mode.

**show tech-support identity mac** *mac-address* **interface** *interface-name*

|                           |   |  |
|---------------------------|---|--|
| <b>Syntax Description</b> | <b>mac</b> <i>mac-address</i>   | Displays information about the client MAC address. |
|                           | <b>interface</b> <i>interface-name</i>  | Displays information about the client interface.   |
| <b>Command Modes</b>      | Privileged EXEC (#)   |  |
| <b>Command History</b>    | <b>Release</b>  | <b>Modification</b>                                |
|                           | Cisco IOS XE Gibraltar 16.10.1  | This command was introduced.                       |
|                           | Cisco IOS XE Gibraltar 16.11.1  |  |
| <b>Usage Guidelines</b>   | <p>The output of the <b>show tech-support platform</b> command is very long. To better manage this output, you can redirect the output to an external file (for example, <b>show tech-support identity mac</b> <i>mac-address</i> <b>interface</b> <i>interface-name</i>   <b>redirect flash:filename</b>) in the local writable storage file system or remote file system.</p> <p>The output of this command displays the following commands:</p> <ul style="list-style-type: none"> <li>• <b>show clock</b></li> <li>• <b>show module</b></li> <li>• <b>show version</b></li> <li>• <b>show switch</b></li> <li>• <b>show redundancy</b></li> <li>• <b>show dot1x statistics</b></li> <li>• <b>show ip access-lists</b></li> <li>• <b>show interface</b></li> <li>• <b>show ip interface brief</b></li> <li>• <b>show vlan brief</b></li> <li>• <b>show running-config</b></li> <li>• <b>show logging</b></li> <li>• <b>show interface controller</b></li> <li>• <b>show platform authentication sbinf</b> interface</li> </ul> |  |

- show platform host-access-table
- show platform pm port-data
- show spanning-tree interface
- show access-session mac detail
- show platform authentication session mac
- show device-tracking database mac details
- show mac address-table address
- show access-session event-logging mac
- show authentication sessions mac details R0
- show ip admission cache R0
- show platform software wired-client R0
- show platform software wired-client F0
- show platform software process database forwarding-manager R0 summary
- show platform software process database forwarding-manager F0 summary
- show platform software object-manager F0 pending-ack-update
- show platform software object-manager F0 pending-issue-update
- show platform software object-manager F0 error-object
- show platform software peer forwarding-manager R0
- show platform software peer forwarding-manager F0
- show platform software VP R0 summary
- show platform software VP F0 summary
- show platform software fed punt cpuq
- show platform software fed punt cause summary
- show platform software fed inject cause summary
- show platform hardware fed fwd-asic drops exceptions
- show platform hardware fed fwd-asic resource tcam table acl
- show platform software fed acl counter hardware
- show platform software fed matm macTable
- show platform software fed ifm mappings
- show platform software trace message fed reverse
- show platform software trace message forwarding-manager R0 reverse
- show platform software trace message forwarding-manager F0 reverse

- show platform software trace message smd R0 reverse
- show authentication sessions mac details
- show platform software wired-client
- show platform software process database forwarding-manager summary
- show platform software object-manager pending-ack-update
- show platform software object-manager pending-issue-update
- show platform software object-manager error-object
- show platform software peer forwarding-manager
- show platform software VP summary
- show platform software trace message forwarding-manager reverse
- show ip admission cache
- show platform software trace message smd reverse
- show platform software fed punt cpuq
- show platform software fed punt cause summary
- show platform software fed inject cause summary
- show platform hardware fed fwd-asic drops exceptions
- show platform hardware fed fwd-asic resource tcam table acl
- show platform software fed acl counter hardware
- show platform software fed matm macTable
- show platform software fed ifm mappings
- show platform software trace message fed reverse

## Examples

The following is sample output from the **show tech-support identity** command:

```
Device# show tech-support identity mac 0000.0001.0003 interface gigabitethernet1/0/1
```

```
.
.
.
```

```
----- show platform software peer forwarding-manager R0 -----
```

IOSD Connection Information:

```
MQIPC (reader) Connection State: Connected, Read-selected
Connections: 1, Failures: 22
3897 packet received (0 dropped), 466929 bytes
Read attempts: 2352, Yields: 0
BIPC Connection state: Connected, Ready
Accepted: 1, Rejected: 0, Closed: 0, Backpressures: 0
36 packets sent, 2808 bytes
```

SMD Connection Information:



```
MQIPC (reader) Connection State: Connected, Read-selected
Connections: 1, Failures: 30
0 packet received (0 dropped), 0 bytes
Read attempts: 1, Yields: 0
MQIPC (writer) Connection State: Connected, Ready
Connections: 1, Failures: 0, Backpressures: 0
0 packet sent, 0 bytes
```

FP Peers Information:

```
Slot: 0
Peer state: connected
OM ID: 0, Download attempts: 638
Complete: 638, Yields: 0, Spurious: 0
IPC Back-Pressure: 0, IPC-Log Back-Pressure: 0
Back-Pressure asserted for IPC: 0, IPC-Log: 1
Number of FP FMAN peer connection expected: 7
Number of FP FMAN online msg received: 1
IPC state: unknown

Config IPC Context:
State: Connected, Read-selected
BIPC Handle: 0xdf3d48e8, BIPC FD: 36, Peer Context: 0xdf3e7158
Tx Packets: 688, Messages: 2392, ACKs: 36
Rx Packets: 37, Bytes: 2068

IPC Log:
Peer name: fman-log-bay0-peer0
Flags: Recovery-Complete
Send Seq: 36, Recv Seq: 36, Msgs Sent: 0, Msgs Recovered: 0

Upstream FMRP IPC Context:
State: Connected, Read-selected
BIPC Handle: 0xdf3e7308, BIPC FD: 37, Peer Context: 0xdf3e7158
TX Packets: 0, Bytes: 0, Drops: 0
Rx Packets: 0, Bytes: 0

Upstream FMRP-IOSd IPC Context:
State: Connected, Read-selected
BIPC Handle: 0xdf3f9c38, BIPC FD: 38, Peer Context: 0xdf3e7158
TX Packets: 0, Bytes: 0, Drops: 0
Rx Packets: 37, Bytes: 2864
Rx ACK Requests: 1, Tx ACK Responses: 1

Upstream FMRP-SMD IPC Context:
State: Connected, Read-selected
BIPC Handle: 0xdf40c568, BIPC FD: 39, Peer Context: 0xdf3e7158
TX Packets: 0, Bytes: 0, Drops: 0
Rx Packets: 0, Bytes: 0
Rx ACK Requests: 0, Tx ACK Responses: 0

Upstream FMRP-WNCD_0 IPC Context:
State: Connected
BIPC Handle: 0xdf4317c8, BIPC FD: 41, Peer Context: 0xdf3e7158
TX Packets: 0, Bytes: 0, Drops: 0
Rx Packets: 0, Bytes: 0
Rx ACK Requests: 0, Tx ACK Responses: 0

Upstream FMRP-WNCMGRD IPC Context:
State: Connected
BIPC Handle: 0xdf41ee98, BIPC FD: 40, Peer Context: 0xdf3e7158
TX Packets: 0, Bytes: 0, Drops: 0
Rx Packets: 0, Bytes: 0
```

```
Rx ACK Requests: 0, Tx ACK Responses: 0

Upstream FMRP-MOBILITYD IPC Context:
  State: Connected
  BIPC Handle: 0xdf4440f8, BIPC FD: 42, Peer Context: 0xdf3e7158
  TX Packets: 0, Bytes: 0, Drops: 0
  Rx Packets: 0, Bytes: 0
  Rx ACK Requests: 0, Tx ACK Responses: 0

Slot: 1
Peer state: connected
  OM ID: 1, Download attempts: 1
    Complete: 1, Yields: 0, Spurious: 0
    IPC Back-Pressure: 0, IPC-Log Back-Pressure: 0
  Back-Pressure asserted for IPC: 0, IPC-Log: 0
  Number of FP FMAN peer connection expected: 7
  Number of FP FMAN online msg received: 1
  IPC state: unknown

Config IPC Context:
  State: Connected, Read-selected
  BIPC Handle: 0xdf45e4d8, BIPC FD: 48, Peer Context: 0xdf470e18
  Tx Packets: 20, Messages: 704, ACKs: 1
  Rx Packets: 2, Bytes: 108

IPC Log:
  Peer name: fman-log-bay0-peer1
  Flags: Recovery-Complete
  Send Seq: 1, Recv Seq: 1, Msgs Sent: 0, Msgs Recovered: 0

Upstream FMRP IPC Context:
  State: Connected, Read-selected
  BIPC Handle: 0xdf470fc8, BIPC FD: 49, Peer Context: 0xdf470e18
  TX Packets: 0, Bytes: 0, Drops: 0
  Rx Packets: 0, Bytes: 0

Upstream FMRP-IOSd IPC Context:
  State: Connected, Read-selected
  BIPC Handle: 0xdf4838f8, BIPC FD: 50, Peer Context: 0xdf470e18
  TX Packets: 0, Bytes: 0, Drops: 0
  Rx Packets: 0, Bytes: 0
  Rx ACK Requests: 0, Tx ACK Responses: 0

Upstream FMRP-SMD IPC Context:
  State: Connected, Read-selected
  BIPC Handle: 0xdf496228, BIPC FD: 51, Peer Context: 0xdf470e18
  TX Packets: 0, Bytes: 0, Drops: 0
  Rx Packets: 0, Bytes: 0
  Rx ACK Requests: 0, Tx ACK Responses: 0

Upstream FMRP-WNCD_0 IPC Context:
  State: Connected
  BIPC Handle: 0xdf4bb488, BIPC FD: 53, Peer Context: 0xdf470e18
  TX Packets: 0, Bytes: 0, Drops: 0
  Rx Packets: 0, Bytes: 0
  Rx ACK Requests: 0, Tx ACK Responses: 0

Upstream FMRP-WNCMGRD IPC Context:
  State: Connected
  BIPC Handle: 0xdf4a8b58, BIPC FD: 52, Peer Context: 0xdf470e18
  TX Packets: 0, Bytes: 0, Drops: 0
  Rx Packets: 0, Bytes: 0
  Rx ACK Requests: 0, Tx ACK Responses: 0
```

```
Upstream FMRP-MOBILITYD IPC Context:
  State: Connected
  BIPC Handle: 0xdf4cddb8, BIPC FD: 54, Peer Context: 0xdf470e18
  TX Packets: 0, Bytes: 0, Drops: 0
  Rx Packets: 0, Bytes: 0
  Rx ACK Requests: 0, Tx ACK Responses: 0
```

----- show platform software peer forwarding-manager R0 -----

IOSD Connection Information:

```
MQIPC (reader) Connection State: Connected, Read-selected
  Connections: 1, Failures: 22
  3897 packet received (0 dropped), 466929 bytes
  Read attempts: 2352, Yields: 0
MQIPC Connection state: Connected, Ready
  Accepted: 1, Rejected: 0, Closed: 0, Backpressures: 0
  36 packets sent, 2808 bytes
```

SMD Connection Information:

```
MQIPC (reader) Connection State: Connected, Read-selected
  Connections: 1, Failures: 30
  0 packet received (0 dropped), 0 bytes
  Read attempts: 1, Yields: 0
MQIPC (writer) Connection State: Connected, Ready
  Connections: 1, Failures: 0, Backpressures: 0
  0 packet sent, 0 bytes
```

FP Peers Information:

```
Slot: 0
  Peer state: connected
  OM ID: 0, Download attempts: 638
  Complete: 638, Yields: 0, Spurious: 0
  IPC Back-Pressure: 0, IPC-Log Back-Pressure: 0
  Back-Pressure asserted for IPC: 0, IPC-Log: 1
  Number of FP FMAN peer connection expected: 7
  Number of FP FMAN online msg received: 1
  IPC state: unknown
```

Config IPC Context:

```
  State: Connected, Read-selected
  BIPC Handle: 0xdf3d48e8, BIPC FD: 36, Peer Context: 0xdf3e7158
  Tx Packets: 688, Messages: 2392, ACKs: 36
  Rx Packets: 37, Bytes: 2068
```

IPC Log:

```
  Peer name: fman-log-bay0-peer0
  Flags: Recovery-Complete
  Send Seq: 36, Recv Seq: 36, Msgs Sent: 0, Msgs Recovered: 0
```

Upstream FMRP IPC Context:

```
  State: Connected, Read-selected
  BIPC Handle: 0xdf3e7308, BIPC FD: 37, Peer Context: 0xdf3e7158
  TX Packets: 0, Bytes: 0, Drops: 0
  Rx Packets: 0, Bytes: 0
```

Upstream FMRP-IOSd IPC Context:

```
  State: Connected, Read-selected
  BIPC Handle: 0xdf3f9c38, BIPC FD: 38, Peer Context: 0xdf3e7158
```

```
TX Packets: 0, Bytes: 0, Drops: 0
Rx Packets: 37, Bytes: 2864
Rx ACK Requests: 1, Tx ACK Responses: 1

Upstream FMRP-SMD IPC Context:
  State: Connected, Read-selected
  BIPC Handle: 0xdf40c568, BIPC FD: 39, Peer Context: 0xdf3e7158
  TX Packets: 0, Bytes: 0, Drops: 0
  Rx Packets: 0, Bytes: 0
  Rx ACK Requests: 0, Tx ACK Responses: 0

Upstream FMRP-WNCD_0 IPC Context:
  State: Connected
  BIPC Handle: 0xdf4317c8, BIPC FD: 41, Peer Context: 0xdf3e7158
  TX Packets: 0, Bytes: 0, Drops: 0
  Rx Packets: 0, Bytes: 0
  Rx ACK Requests: 0, Tx ACK Responses: 0

Upstream FMRP-WNCMGRD IPC Context:
  State: Connected
  BIPC Handle: 0xdf41ee98, BIPC FD: 40, Peer Context: 0xdf3e7158
  TX Packets: 0, Bytes: 0, Drops: 0
  Rx Packets: 0, Bytes: 0
  Rx ACK Requests: 0, Tx ACK Responses: 0

Upstream FMRP-MOBILITYD IPC Context:
  State: Connected
  BIPC Handle: 0xdf4440f8, BIPC FD: 42, Peer Context: 0xdf3e7158
  TX Packets: 0, Bytes: 0, Drops: 0
  Rx Packets: 0, Bytes: 0
  Rx ACK Requests: 0, Tx ACK Responses: 0

Slot: 1
Peer state: connected
  OM ID: 1, Download attempts: 1
    Complete: 1, Yields: 0, Spurious: 0
    IPC Back-Pressure: 0, IPC-Log Back-Pressure: 0
  Back-Pressure asserted for IPC: 0, IPC-Log: 0
  Number of FP FMAN peer connection expected: 7
  Number of FP FMAN online msg received: 1
  IPC state: unknown

Config IPC Context:
  State: Connected, Read-selected
  BIPC Handle: 0xdf45e4d8, BIPC FD: 48, Peer Context: 0xdf470e18
  Tx Packets: 20, Messages: 704, ACKs: 1
  Rx Packets: 2, Bytes: 108

IPC Log:
  Peer name: fman-log-bay0-peer1
  Flags: Recovery-Complete
  Send Seq: 1, Recv Seq: 1, Msgs Sent: 0, Msgs Recovered: 0

Upstream FMRP IPC Context:
  State: Connected, Read-selected
  BIPC Handle: 0xdf470fc8, BIPC FD: 49, Peer Context: 0xdf470e18
  TX Packets: 0, Bytes: 0, Drops: 0
  Rx Packets: 0, Bytes: 0

Upstream FMRP-IOSd IPC Context:
  State: Connected, Read-selected
  BIPC Handle: 0xdf4838f8, BIPC FD: 50, Peer Context: 0xdf470e18
  TX Packets: 0, Bytes: 0, Drops: 0
  Rx Packets: 0, Bytes: 0
```

Rx ACK Requests: 0, Tx ACK Responses: 0

Upstream FMRP-SMD IPC Context:

State: Connected, Read-selected  
 BIPC Handle: 0xdf496228, BIPC FD: 51, Peer Context: 0xdf470e18  
 TX Packets: 0, Bytes: 0, Drops: 0  
 Rx Packets: 0, Bytes: 0  
 Rx ACK Requests: 0, Tx ACK Responses: 0

Upstream FMRP-WNCD\_0 IPC Context:

State: Connected  
 BIPC Handle: 0xdf4bb488, BIPC FD: 53, Peer Context: 0xdf470e18  
 TX Packets: 0, Bytes: 0, Drops: 0  
 Rx Packets: 0, Bytes: 0  
 Rx ACK Requests: 0, Tx ACK Responses: 0

Upstream FMRP-WNCMGRD IPC Context:

State: Connected  
 BIPC Handle: 0xdf4a8b58, BIPC FD: 52, Peer Context: 0xdf470e18  
 TX Packets: 0, Bytes: 0, Drops: 0  
 Rx Packets: 0, Bytes: 0  
 Rx ACK Requests: 0, Tx ACK Responses: 0

Upstream FMRP-MOBILITYD IPC Context:

State: Connected  
 BIPC Handle: 0xdf4cddb8, BIPC FD: 54, Peer Context: 0xdf470e18  
 TX Packets: 0, Bytes: 0, Drops: 0  
 Rx Packets: 0, Bytes: 0  
 Rx ACK Requests: 0, Tx ACK Responses: 0

----- show platform software VP R0 summary -----

Forwarding Manager Vlan Port Information

| Vlan | Intf-ID | Stp-state  |
|------|---------|------------|
| 1    | 7       | Forwarding |
| 1    | 9       | Forwarding |
| 1    | 17      | Forwarding |
| 1    | 27      | Forwarding |
| 1    | 28      | Forwarding |
| 1    | 29      | Forwarding |
| 1    | 30      | Forwarding |
| 1    | 31      | Forwarding |
| 1    | 40      | Forwarding |
| 1    | 41      | Forwarding |

Forwarding Manager Vlan Port Information

| Vlan | Intf-ID | Stp-state  |
|------|---------|------------|
| 1    | 49      | Forwarding |
| 1    | 51      | Forwarding |
| 1    | 63      | Forwarding |
| 1    | 72      | Forwarding |
| 1    | 73      | Forwarding |
| 1    | 74      | Forwarding |

----- show platform software VP R0 summary -----

Forwarding Manager Vlan Port Information

| Vlan | Intf-ID | Stp-state  |
|------|---------|------------|
| 1    | 7       | Forwarding |
| 1    | 9       | Forwarding |
| 1    | 17      | Forwarding |
| 1    | 27      | Forwarding |
| 1    | 28      | Forwarding |
| 1    | 29      | Forwarding |
| 1    | 30      | Forwarding |
| 1    | 31      | Forwarding |
| 1    | 40      | Forwarding |
| 1    | 41      | Forwarding |

Forwarding Manager Vlan Port Information

| Vlan | Intf-ID | Stp-state  |
|------|---------|------------|
| 1    | 49      | Forwarding |
| 1    | 51      | Forwarding |
| 1    | 63      | Forwarding |
| 1    | 72      | Forwarding |
| 1    | 73      | Forwarding |
| 1    | 74      | Forwarding |

.  
.  
.

# 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*]

|                           |  |
|---------------------------|--|
| <b>Syntax Description</b> | <i>map-name</i> (Optional) Name of a specific VLAN access map. |
|---------------------------|--|

|                      |                     |
|----------------------|---------------------|
| <b>Command Modes</b> | Privileged EXEC (#) |
|----------------------|---------------------|

|                        |                             |                              |
|------------------------|-----------------------------|------------------------------|
| <b>Command History</b> | <b>Release</b>              | <b>Modification</b>          |
|                        | Cisco IOS XE Everest 16.6.1 | This command was introduced. |

## Examples

The following is sample output from the **show vlan access-map** command:

```
Device# show vlan access-map

Vlan access-map "vmap4" 10
  Match clauses:
    ip address: a12
  Action:
    forward
Vlan access-map "vmap4" 20
  Match clauses:
    ip address: a12
  Action:
    forward
```

# show vlan filter

To display information about all VLAN filters or about a particular VLAN or VLAN access map, use the **show vlan filter** command in privileged EXEC mode.

**show vlan filter** {**access-map** *name* | **vlan** *vlan-id*}

|                           |                               |   |
|---------------------------|-------------------------------|---|
| <b>Syntax Description</b> | <b>access-map</b> <i>name</i> | (Optional) Displays filtering information for the specified VLAN access map.              |
|                           | <b>vlan</b> <i>vlan-id</i>    | (Optional) Displays filtering information for the specified VLAN. The range is 1 to 4094. |
| <b>Command Modes</b>      | Privileged EXEC (#)           |   |
| <b>Command History</b>    | <b>Release</b>                | <b>Modification</b>   |
|                           | Cisco IOS XE Everest 16.6.1   | This command was introduced.  |

## Examples

The following is sample 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**]}]

|                           |   |  |
|---------------------------|---|--|
| <b>Syntax Description</b> | <b>group-name</b> <i>vlan-group-name</i>  | (Optional) Displays the VLANs mapped to the specified VLAN group.                      |
|                           | <b>user_count</b>   | (Optional) Displays the number of users in each VLAN mapped to a specified VLAN group. |
| <b>Command Modes</b>      | Privileged EXEC (#)   |  |
| <b>Command History</b>    | <b>Release</b>  | <b>Modification</b>  |
|                           | Cisco IOS XE Everest 16.6.1   | This command was introduced.   |
| <b>Usage Guidelines</b>   | The <b>show vlan group</b> command displays the existing VLAN groups and lists the VLANs and VLAN ranges that are members of each VLAN group. If you enter the <b>group-name</b> keyword, only the members of the specified VLAN group are displayed. |  |

## Examples

This example shows how to display the members of a specified VLAN group:

```
Device# show vlan group group-name group2
vlan group group1 :40-45
```

This example shows how to display number of users in each of the VLANs in a group:

```
Device# show vlan group group-name group2 user_count
```

```

VLAN      : Count
-----
40        : 5
41        : 8
42        : 12
43        : 2
44        : 9
45        : 0
```

# switchport port-security aging

To set the aging time and type for secure address entries or to change the aging behavior for secure addresses on a particular port, use the **switchport port-security aging** command in interface configuration mode. To disable port security aging or to set the parameters to their default states, use the **no** form of this command.

**switchport port-security aging** {static | time *time* | type {absolute | inactivity}}  
**no switchport port-security aging** {static | time | type}

## Syntax Description

|                            |  |
|----------------------------|--|
| <b>static</b>              | Enables aging for statically configured secure addresses on this port.   |
| <b>time</b><br><i>time</i> | Specifies the aging time for this port. The range is 0 to 1440 minutes. If the time is 0, aging is disabled for this port.   |
| <b>type</b>                | Sets the aging type.   |
| <b>absolute</b>            | Sets absolute aging type. All the secure addresses on this port age out exactly after the time (minutes) specified and are removed from the secure address list.         |
| <b>inactivity</b>          | Sets the inactivity aging type. The secure addresses on this port age out only if there is no data traffic from the secure source address for the specified time period. |

## Command Default

The port security aging feature is disabled. The default time is 0 minutes.  
 The default aging type is absolute.  
 The default static aging behavior is disabled.

## Command Modes

Interface configuration (config-if)

## Command History

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

## Usage Guidelines

To enable secure address aging for a particular port, set the aging time to a value other than 0 for that port.

To allow limited time access to particular secure addresses, set the aging type as **absolute**. When the aging time lapses, the secure addresses are deleted.

To allow continuous access to a limited number of secure addresses, set the aging type as **inactivity**. This removes the secure address when it become inactive, and other addresses can become secure.

To allow unlimited access to a secure address, configure it as a secure address, and disable aging for the statically configured secure address by using the **no switchport port-security aging static** interface configuration command.

This example sets the aging time as 2 hours for absolute aging for all the secure addresses on the port:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# switchport port-security aging time 120
```

```
Device(config-if)# end
```

This example sets the aging time as 2 minutes for inactivity aging type with aging enabled for configured secure addresses on the port:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# switchport port-security aging time 2
Device(config-if)# switchport port-security aging type inactivity
Device(config-if)# switchport port-security aging static
Device(config-if)# end
```

This example shows how to disable aging for configured secure addresses:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# no switchport port-security aging static
Device(config-if)# end
```

# switchport port-security mac-address

To configure secure MAC addresses or sticky MAC address learning, use the **switchport port-security mac-address** interface configuration command. To return to the default setting, use the **no** form of this command.

```
switchport port-security mac-address {mac-address [{vlan {vlan-id {access | voice}}]} | sticky
[{mac-address | vlan {vlan-id {access | voice}}]}]
no switchport port-security mac-address {mac-address [{vlan {vlan-id {access | voice}}]} | sticky
[{mac-address | vlan {vlan-id {access | voice}}]}]
```

## Syntax Description

|                     |  |
|---------------------|--|
| <b>mac-address</b>  | A secure MAC address for the interface by entering a 48-bit MAC address. You can add additional secure MAC addresses up to the maximum value configured.   |
| <b>vlan vlan-id</b> | (Optional) On a trunk port only, specifies the VLAN ID and the MAC address. If no VLAN ID is specified, the native VLAN is used.   |
| <b>vlan access</b>  | (Optional) On an access port only, specifies the VLAN as an access VLAN.   |
| <b>vlan voice</b>   | (Optional) On an access port only, specifies the VLAN as a voice VLAN.   |
| <b>Note</b>         | The <b>voice</b> keyword is available only if voice VLAN is configured on a port and if that port is not the access VLAN.  |
| <b>sticky</b>       | Enables the interface for sticky learning. When sticky learning is enabled, the interface adds all secure MAC addresses that are dynamically learned to the running configuration and converts these addresses to sticky secure MAC addresses. |
| <b>mac-address</b>  | (Optional) A MAC address to specify a sticky secure MAC address.   |

## Command Default

No secure MAC addresses are configured.  
Sticky learning is disabled.

## Command Modes

Interface configuration (config-if)

## Command History

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

## Usage Guidelines

A secure port has the following limitations:

- A secure port can be an access port or a trunk port; it cannot be a dynamic access port.
- A secure port cannot be a routed port.
- A secure port cannot be a protected port.
- A secure port cannot be a destination port for Switched Port Analyzer (SPAN).
- A secure port cannot belong to a Gigabit or 10-Gigabit EtherChannel port group.

- You cannot configure static secure or sticky secure MAC addresses in the voice VLAN.
- When you enable port security on an interface that is also configured with a voice VLAN, set the maximum allowed secure addresses on the port to two. When the port is connected to a Cisco IP phone, the IP phone requires one MAC address. The Cisco IP phone address is learned on the voice VLAN, but is not learned on the access VLAN. If you connect a single PC to the Cisco IP phone, no additional MAC addresses are required. If you connect more than one PC to the Cisco IP phone, you must configure enough secure addresses to allow one for each PC and one for the Cisco IP phone.
- Voice VLAN is supported only on access ports and not on trunk ports.

Sticky secure MAC addresses have these characteristics:

- When you enable sticky learning on an interface by using the **switchport port-security mac-address sticky** interface configuration command, the interface converts all the dynamic secure MAC addresses, including those that were dynamically learned before sticky learning was enabled, to sticky secure MAC addresses and adds all sticky secure MAC addresses to the running configuration.
- If you disable sticky learning by using the **no switchport port-security mac-address sticky** interface configuration command or the running configuration is removed, the sticky secure MAC addresses remain part of the running configuration but are removed from the address table. The addresses that were removed can be dynamically reconfigured and added to the address table as dynamic addresses.
- When you configure sticky secure MAC addresses by using the **switchport port-security mac-address sticky mac-address** interface configuration command, these addresses are added to the address table and the running configuration. If port security is disabled, the sticky secure MAC addresses remain in the running configuration.
- If you save the sticky secure MAC addresses in the configuration file, when the device restarts or the interface shuts down, the interface does not need to relearn these addresses. If you do not save the sticky secure addresses, they are lost. If sticky learning is disabled, the sticky secure MAC addresses are converted to dynamic secure addresses and are removed from the running configuration.
- If you disable sticky learning and enter the **switchport port-security mac-address sticky mac-address** interface configuration command, an error message appears, and the sticky secure MAC address is not added to the running configuration.

You can verify your settings by using the **show port-security** command.

This example shows how to configure a secure MAC address and a VLAN ID on a port:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 2/0/2
Device(config-if)# switchport mode trunk
Device(config-if)# switchport port-security
Device(config-if)# switchport port-security mac-address 1000.2000.3000 vlan 3
Device(config-if)# end
```

This example shows how to enable sticky learning and to enter two sticky secure MAC addresses on a port:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 2/0/2
Device(config-if)# switchport port-security mac-address sticky
Device(config-if)# switchport port-security mac-address sticky 0000.0000.4141
```

```
Device(config-if)# switchport port-security mac-address sticky 0000.0000.000f
Device(config-if)# end
```

## switchport port-security maximum

To configure the maximum number of secure MAC addresses, use the **switchport port-security maximum** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

**switchport port-security maximum** *value* [**vlan** [{*vlan-list* | [{**access** | **voice**}]}]]  
**no switchport port-security maximum** *value* [**vlan** [{*vlan-list* | [{**access** | **voice**}]}]]

### Syntax Description

|                  |  |
|------------------|--|
| <i>value</i>     | Sets the maximum number of secure MAC addresses for the interface.<br><br>The default setting is 1.  |
| <b>vlan</b>      | (Optional) For trunk ports, sets the maximum number of secure MAC addresses on a VLAN or range of VLANs. If the <b>vlan</b> keyword is not entered, the default value is used. |
| <i>vlan-list</i> | (Optional) Range of VLANs separated by a hyphen or a series of VLANs separated by commas. For nonspecified VLANs, the per-VLAN maximum value is used.                          |
| <b>access</b>    | (Optional) On an access port only, specifies the VLAN as an access VLAN.   |
| <b>voice</b>     | (Optional) On an access port only, specifies the VLAN as a voice VLAN.   |
| <b>Note</b>      | The <b>voice</b> keyword is available only if voice VLAN is configured on a port and if that port is not the access VLAN.  |

### Command Default

When port security is enabled and no keywords are entered, the default maximum number of secure MAC addresses is 1.

### Command Modes

Interface configuration (config-if)

### Command History

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

### Usage Guidelines

The maximum number of secure MAC addresses that you can configure on a device is set by the maximum number of available MAC addresses allowed in the system. This number is determined by the active Switch Database Management (SDM) template. See the **sdm prefer** command. This number represents the total of available MAC addresses, including those used for other Layer 2 functions and any other secure MAC addresses configured on interfaces.

A secure port has the following limitations:

- A secure port can be an access port or a trunk port; it cannot be a dynamic access port.
- A secure port cannot be a routed port.
- A secure port cannot be a protected port.
- A secure port cannot be a destination port for Switched Port Analyzer (SPAN).
- A secure port cannot belong to a Gigabit or 10-Gigabit EtherChannel port group.

- When you enable port security on an interface that is also configured with a voice VLAN, set the maximum allowed secure addresses on the port to two. When the port is connected to a Cisco IP phone, the IP phone requires one MAC address. The Cisco IP phone address is learned on the voice VLAN, but is not learned on the access VLAN. If you connect a single PC to the Cisco IP phone, no additional MAC addresses are required. If you connect more than one PC to the Cisco IP phone, you must configure enough secure addresses to allow one for each PC and one for the Cisco IP phone.

Voice VLAN is supported only on access ports and not on trunk ports.

- When you enter a maximum secure address value for an interface, if the new value is greater than the previous value, the new value overrides the previously configured value. If the new value is less than the previous value and the number of configured secure addresses on the interface exceeds the new value, the command is rejected.

Setting a maximum number of addresses to one and configuring the MAC address of an attached device ensures that the device has the full bandwidth of the port.

When you enter a maximum secure address value for an interface, this occurs:

- If the new value is greater than the previous value, the new value overrides the previously configured value.
- If the new value is less than the previous value and the number of configured secure addresses on the interface exceeds the new value, the command is rejected.

You can verify your settings by using the **show port-security** command.

This example shows how to enable port security on a port and to set the maximum number of secure addresses to 5. The violation mode is the default, and no secure MAC addresses are configured.

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 2/0/2
Device(config-if)# switchport mode access
Device(config-if)# switchport port-security
Device(config-if)# switchport port-security maximum 5
Device(config-if)# end
```



## switchport port-security violation

To configure secure MAC address violation mode or the action to be taken if port security is violated, use the **switchport port-security violation** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

```
switchport port-security violation {protect | restrict | shutdown | shutdown vlan}
no switchport port-security violation {protect | restrict | shutdown | shutdown vlan}
```

|                           |  |  |
|---------------------------|--|--|
| <b>Syntax Description</b> | <b>protect</b>   | Sets the security violation protect mode.              |
|                           | <b>restrict</b>  | Sets the security violation restrict mode.             |
|                           | <b>shutdown</b>  | Sets the security violation shutdown mode.             |
|                           | <b>shutdown vlan</b>   | Sets the security violation mode to per-VLAN shutdown. |
| <b>Command Default</b>    | The default violation mode is <b>shutdown</b> .  |  |
| <b>Command Modes</b>      | Interface configuration (config-if)  |  |
| <b>Command History</b>    | <b>Release</b>   | <b>Modification</b>                                    |
|                           | Cisco IOS XE Everest 16.6.1  | This command was introduced.                           |
| <b>Usage Guidelines</b>   | In the security violation protect mode, when the number of port secure MAC addresses reaches the maximum limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses to drop below the maximum value or increase the number of maximum allowable addresses. You are not notified that a security violation has occurred. |  |



**Note** We do not recommend configuring the protect mode on a trunk port. The protect mode disables learning when any VLAN reaches its maximum limit, even if the port has not reached its maximum limit.

In the security violation restrict mode, when the number of secure MAC addresses reaches the limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses or increase the number of maximum allowable addresses. An SNMP trap is sent, a syslog message is logged, and the violation counter increments.

In the security violation shutdown mode, the interface is error-disabled when a violation occurs and the port LED turns off. An SNMP trap is sent, a syslog message is logged, and the violation counter increments. When a secure port is in the error-disabled state, you can bring it out of this state by entering the **errdisable recovery cause psecure-violation** global configuration command, or you can manually re-enable it by entering the **shutdown** and **no shutdown** interface configuration commands.

When the security violation mode is set to per-VLAN shutdown, only the VLAN on which the violation occurred is error-disabled.

A secure port has the following limitations:

- A secure port can be an access port or a trunk port; it cannot be a dynamic access port.
- A secure port cannot be a routed port.
- A secure port cannot be a protected port.
- A secure port cannot be a destination port for Switched Port Analyzer (SPAN).
- A secure port cannot belong to a Gigabit or 10-Gigabit EtherChannel port group.

A security violation occurs when the maximum number of secure MAC addresses are in the address table and a station whose MAC address is not in the address table attempts to access the interface or when a station whose MAC address is configured as a secure MAC address on another secure port attempts to access the interface.

When a secure port is in the error-disabled state, you can bring it out of this state by entering the **errdisable recovery cause psecure-violation** global configuration command. You can manually re-enable the port by entering the **shutdown** and **no shutdown** interface configuration commands or by using the **clear errdisable interface** privileged EXEC command.

You can verify your settings by using the **show port-security** privileged EXEC command.

This example shows how to configure a port to shut down only the VLAN if a MAC security violation occurs:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet2/0/2
Device(config)# switchport port-security violation shutdown vlan
Device(config)# exit
```

## tacacs server

To configure the TACACS+ server for IPv6 or IPv4 and enter TACACS+ server configuration mode, use the **tacacs server** command in global configuration mode. To remove the configuration, use the **no** form of this command.

**tacacs server** *name*  
**no tacacs server**

### Syntax Description

|             |  |
|-------------|--|
| <i>name</i> | Name of the private TACACS+ server host. |
|-------------|--|

### Command Default

No TACACS+ server is configured.

### Command Modes

Global configuration (config)

### Command History

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

### Usage Guidelines

The **tacacs server** command configures the TACACS server using the *name* argument and enters TACACS+ server configuration mode. The configuration is applied once you have finished configuration and exited TACACS+ server configuration mode.

### Examples

The following example shows how to configure the TACACS server using the name server1 and enter TACACS+ server configuration mode to perform further configuration:

```
Device> enable
Device# configure terminal
Device(config)# tacacs server server1
Device(config-server-tacacs)# end
```

### Related Commands

| Command                            | Description   |
|------------------------------------|---|
| <b>address ipv6 (TACACS+)</b>      | Configures the IPv6 address of the TACACS+ server.                                      |
| <b>key (TACACS+)</b>               | Configures the per-server encryption key on the TACACS+ server.                         |
| <b>port (TACACS+)</b>              | Specifies the TCP port to be used for TACACS+ connections.                              |
| <b>send-nat-address (TACACS+)</b>  | Sends a client's post-NAT address to the TACACS+ server.                                |
| <b>single-connection (TACACS+)</b> | Enables all TACACS packets to be sent to the same server using a single TCP connection. |
| <b>timeout(TACACS+)</b>            | Configures the time to wait for a reply from the specified TACACS server.               |

## tracking (IPv6 snooping)

To override the default tracking policy on a port, use the **tracking** command in IPv6 snooping policy configuration mode.

**tracking** {**enable** [**reachable-lifetime** {*value* | **infinite**}] | **disable** [**stale-lifetime** {*value* | **infinite**}]}

| Syntax Description        |   |                              |
|---------------------------|---|------------------------------|
| <b>enable</b>             | Enables tracking.   |                              |
| <b>reachable-lifetime</b> | (Optional) Specifies the maximum amount of time a reachable entry is considered to be directly or indirectly reachable without proof of reachability. <ul style="list-style-type: none"> <li>The <b>reachable-lifetime</b> keyword can be used only with the <b>enable</b> keyword.</li> <li>Use of the <b>reachable-lifetime</b> keyword overrides the global reachable lifetime configured by the <b>ipv6 neighbor binding reachable-lifetime</b> command.</li> </ul> |                              |
| <i>value</i>              | Lifetime value, in seconds. The range is from 1 to 86400, and the default is 300.   |                              |
| <b>infinite</b>           | Keeps an entry in a reachable or stale state for an infinite amount of time.  |                              |
| <b>disable</b>            | Disables tracking.  |                              |
| <b>stale-lifetime</b>     | (Optional) Keeps the time entry in a stale state, which overwrites the global stale-lifetime configuration. <ul style="list-style-type: none"> <li>The stale lifetime is 86,400 seconds.</li> <li>The <b>stale-lifetime</b> keyword can be used only with the <b>disable</b> keyword.</li> <li>Use of the <b>stale-lifetime</b> keyword overrides the global stale lifetime configured by the <b>ipv6 neighbor binding stale-lifetime</b> command.</li> </ul>           |                              |
| <b>Command Default</b>    | The time entry is kept in a reachable state.  |                              |
| <b>Command Modes</b>      | IPv6 snooping configuration (config-ipv6-snooping)  |                              |
| <b>Command History</b>    | <b>Release</b>  | <b>Modification</b>          |
|                           | Cisco IOS XE Everest 16.6.1   | This command was introduced. |

---

### Usage Guidelines

The **tracking** command overrides the default tracking policy set by the **ipv6 neighbor tracking** command on the port on which this policy applies. This function is useful on trusted ports where, for example, you may not want to track entries but want an entry to stay in the binding table to prevent it from being stolen.

The **reachable-lifetime** keyword is the maximum time an entry will be considered reachable without proof of reachability, either directly through tracking or indirectly through IPv6 snooping. After the **reachable-lifetime** value is reached, the entry is moved to stale. Use of the **reachable-lifetime** keyword with the tracking command overrides the global reachable lifetime configured by the **ipv6 neighbor binding reachable-lifetime** command.

The **stale-lifetime** keyword is the maximum time an entry is kept in the table before it is deleted or the entry is proven to be reachable, either directly or indirectly. Use of the **reachable-lifetime** keyword with the **tracking** command overrides the global stale lifetime configured by the **ipv6 neighbor binding stale-lifetime** command.

This example shows how to define an IPv6 snooping policy name as `policy1` and configures an entry to stay in the binding table for an infinite length of time on a trusted port:

```
Device> enable
Device# configure terminal
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# tracking disable stale-lifetime infinite
Device(config-ipv6-snooping)# end
```

# 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 (config-nd-inspection)  
 IPv6 snooping configuration (config-ipv6-snooping)

| Command History | Release                     | Modification                 |
|-----------------|-----------------------------|------------------------------|
|                 | Cisco IOS XE Everest 16.6.1 | 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, and configures the port to be trusted:

```
Device> enable
Device# configure terminal
Device(config)# ipv6 nd inspection policy1
Device(config-nd-inspection)# trusted-port
Device(config-nd-inspection)# end
```

This example shows how to define an IPv6 snooping policy name as policy1, and configures the port to be trusted:

```
Device> enable
Device# configure terminal
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# trusted-port
Device(config-ipv6-snooping)# end
```

# username

To establish the username-based authentication system, use the **username** command in global configuration mode. To remove an established username-based authentication, use the **no** form of this command.

```
username name [aaa attribute list aaa-list-name]
username name [access-class access-list-number]
username name [algorithm-type {md5 | scrypt | sha256}]
username name [autocommand command]
username name [callback-dialstring telephone-number]
username name [callback-line [tty] line-number [ending-line-number]]
username name [callback-rotary rotary-group-number]
username name [common-criteria-policy policy-name]
username name [dnis]
username name [mac]
username name [nocallback-verify]
username name [noescape]
username name [nohangup]
username name [{nopassword | password password | password encryption-type encrypted-password}]
username name [one-time {password {0 | 6 | 7} password} | secret {0 | 5 | 8 | 9} password}]
username name [password secret]
username name [privilege level]
username name [secret {0 | 5} password]
username name [serial-number]
username name [user-maxlinks number]
username name [view view-name]
no username name
```

## Syntax Description

|   |  |
|---|--|
| <i>name</i>                                       | Hostname, server name, user ID, or command name. The <i>name</i> argument can be only one word. Blank spaces and quotation marks are not allowed.  |
| <b>aaa attribute list</b><br><i>aaa-list-name</i> | (Optional) Uses the specified authentication, authorization, and accounting (AAA) method list.   |
| <b>access-class</b><br><i>access-list-number</i>  | (Optional) Specifies an outgoing access list that overrides the access list specified in the <b>access-class</b> command that is available in line configuration mode. It is used for the duration of the user's session.  |
| <b>algorithm-type</b>                             | (Optional) Specifies the algorithm to use for hashing the plaintext secret for the user. <ul style="list-style-type: none"> <li>• <b>md5</b>: Encodes the password using the MD5 algorithm.</li> <li>• <b>scrypt</b>: Encodes the password using the SCRYPT hashing algorithm.</li> <li>• <b>sha256</b>: Encodes the password using the PBKDF2 hashing algorithm.</li> </ul> |

|   |  |
|---|--|
| <b>autocommand</b> <i>command</i>                     | (Optional) Causes the specified <b>autocommand</b> command to be issued automatically after the user logs in. When the specified <b>autocommand</b> command is complete, the session is terminated. Because the command can be of any length and can contain embedded spaces, commands using the <b>autocommand</b> keyword must be the last option on the line. |
| <b>callback-dialstring</b><br><i>telephone-number</i> | (Optional) Permits you to specify a telephone number to pass to the Data Circuit-terminating Equipment (DCE) device; for asynchronous callback only.   |
| <b>callback-line</b> <i>line-number</i>               | (Optional) Specifies relative number of the terminal line (or the first line in a contiguous group) on which you enable a specific username for callback; for asynchronous callback only. Numbering begins with zero.  |
| <i>ending-line-number</i>                             | (Optional) Relative number of the last line in a contiguous group on which you want to enable a specific username for callback. If you omit the keyword (such as <b>tty</b> ), then line number and ending line number are absolute rather than relative line numbers.   |
| <b>tty</b>  | (Optional) Specifies standard asynchronous line; for asynchronous callback only.   |
| <b>callback-rotary</b><br><i>rotary-group-number</i>  | (Optional) Permits you to specify a rotary group number on which you want to enable a specific username for callback; for asynchronous callback only. The next available line in the rotary group is selected. Range: 1 to 100.  |
| <b>common-criteria-policy</b>                         | (Optional) Specifies the name of the common criteria policy.   |
| <b>dnis</b>   | (Optional) Does not require a password when obtained through the Dialed Number Identification Service (DNIS).  |
| <b>mac</b>  | (Optional) Allows a MAC address to be used as the username for MAC filtering done locally.   |
| <b>nocallback-verify</b>                              | (Optional) Specifies that authentication is not required for EXEC callback on the specified line.  |
| <b>noescape</b>                                       | (Optional) Prevents the user from using an escape character on the host to which that user is connected.   |
| <b>nohangup</b>                                       | (Optional) Prevents Cisco IOS software from disconnecting the user after an automatic command (set up with the <b>autocommand</b> keyword) is run. Instead, the user gets another user EXEC prompt.  |
| <b>nopassword</b>                                     | (Optional) No password is required for the user to log in. This is usually the most useful keyword to use in combination with the <b>autocommand</b> keyword.  |
| <b>password</b>                                       | (Optional) Specifies a password to access the <i>name</i> argument. The password must be from 1 to 25 characters, can contain embedded spaces, and must be the last option specified in the <b>username</b> command.   |
| <i>password</i>                                       | Password that the user enters.   |



|   |  |
|---|--|
| <i>encryption-type</i>                  | Single-digit number that defines whether the text immediately following the <b>password</b> is encrypted, and if so, what type of encryption is used. Defined encryption types are 0, which means that the text immediately following the <b>password</b> is not encrypted, and 6 and 7, which means that the text is encrypted using a Cisco-defined encryption algorithm.  |
| <i>encrypted-password</i>               | Encrypted password that the user enters.   |
| <b>one-time</b>                         | (Optional) Specifies that the username and password is valid for only one time. This configuration is used to prevent default credentials from remaining in user configurations. <ul style="list-style-type: none"> <li>• <b>0</b>: Specifies that an unencrypted password or secret (depending on the configuration) follows.</li> <li>• <b>6</b>: Specifies that an encrypt password follows.</li> <li>• <b>7</b>: Specifies that a hidden password follows.</li> <li>• <b>5</b>: Specifies that a MD5 HASHED secret follows.</li> <li>• <b>8</b>: Specifies that a PBKDF2 HASHED secret follows.</li> <li>• <b>9</b>: Specifies that a SCRYPT HASHED secret follows.</li> </ul> |
| <b>secret</b>                           | (Optional) Specifies a secret for the user.  |
| <i>secret</i>                           | For Challenge Handshake Authentication Protocol (CHAP) authentication. Specifies the secret for the local device or the remote device. The secret is encrypted when it is stored on the local device. The secret can consist of any string of up to 11 ASCII characters. There is no limit to the number of username and password combinations that can be specified, allowing any number of remote devices to be authenticated.   |
| <b>privilege</b> <i>privilege-level</i> | (Optional) Sets the privilege level for the user. Range: 1 to 15.  |
| <b>serial-number</b>                    | (Optional) Specifies the serial number.  |
| <b>user-maxlinks</b> <i>number</i>      | (Optional) Specifies the maximum number of inbound links allowed for the user.   |
| <b>view</b> <i>view-name</i>            | (Optional) Associates a CLI view name, which is specified with the <b>parser view</b> command, with the local AAA database; for CLI view only.   |

**Command Default**

No username-based authentication system is established.

**Command Modes**

Global configuration (config)

**Command History****Release**

Cisco IOS XE Everest 16.6.1

**Modi**This c  
intro**Usage Guidelines**The **username** command provides username or password authentication, or both, for login purposes only.

Multiple **username** commands can be used to specify options for a single user.

Add a username entry for each remote system with which the local device communicates, and from which it requires authentication. The remote device must have a username entry for the local device. This entry must have the same password as the local device's entry for that remote device.

This command can be useful for defining usernames that get special treatment. For example, you can use this command to define an *info* username that does not require a password, but connects the user to a general purpose information service.

The **username** command is required as part of the configuration for CHAP. Add a username entry for each remote system from which the local device requires authentication.

To enable the local device to respond to remote CHAP challenges, one **username name** entry must be the same as the **hostname** entry that has already been assigned to the other device. To avoid the situation of a privilege level 1 user entering into a higher privilege level, configure a per-user privilege level other than 1, for example, 0 or 2 through 15. Per-user privilege levels override virtual terminal privilege levels.

### CLI and Lawful Intercept Views

Both CLI views and lawful intercept views restrict access to specified commands and configuration information. A lawful intercept view allows the user to secure access to lawful intercept commands that are held within the TAP-MIB, which is a special set of SNMP commands that store information about calls and users.

Users who are specified via the **lawful-intercept** keyword are placed in the lawful-intercept view by default if no other privilege level or view name is explicitly specified.

If no value is specified for the *secret* argument, and the **debug serial-interface** command is enabled, an error is displayed when a link is established and the CHAP challenge is not implemented. The CHAP debugging information is available using the **debug ppp negotiation**, **debug serial-interface**, and **debug serial-packet** commands.

## Examples

The following example shows how to implement a service similar to the UNIX **who** command, which can be entered at the login prompt, and lists the current users of the device:

```
Device> enable
Device# configure terminal
Device(config)# username who nopassword nohangup autocommand show users
```

The following example shows how to implement an information service that does not require a password to be used:

```
Device> enable
Device# configure terminal
Device(config)# username info nopassword noescape autocommand telnet nic.ddn.mil
```

The following example shows how to implement an ID that works even if all the TACACS+ servers break:

```
Device> enable
Device# configure terminal
Device(config)# username superuser password superpassword
```

The following example shows how to enable CHAP on interface serial 0 of server\_1. It also defines a password for a remote server named server\_r.

```
hostname server_1
```

```
username server_r password theirsystm
interface serial 0
 encapsulation ppp
 ppp authentication chap
```

The following is a sample output from the **show running-config** command displaying the passwords that are encrypted:

```
hostname server_l
username server_r password 7 121F0A18
interface serial 0
 encapsulation ppp
 ppp authentication chap
```

The following example shows how a privilege level 1 user is denied access to privilege levels higher than 1:

```
Device> enable
Device# configure terminal
Device(config)# username user privilege 0 password 0 cisco
Device(config)# username user2 privilege 2 password 0 cisco
```

The following example shows how to remove username-based authentication for user2:

```
Device> enable
Device# configure terminal
Device(config)# no username user2
```

#### Related Commands

| Command                       | Description  |
|-------------------------------|--|
| <b>debug ppp negotiation</b>  | Displays PPP packets sent during PPP startup, where PPP op   |
| <b>debug serial-interface</b> | Displays information about a serial connection failure.  |
| <b>debug serial-packet</b>    | Displays more detailed serial interface debugging information using the <b>debug serial interface</b> command. |

# 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 device. To delete a VLAN map entry, use the **no** form of this command.

**vlan access-map** *name* [*number*]  
**no vlan access-map** *name* [*number*]

|                           |   |   |
|---------------------------|---|---|
| <b>Syntax Description</b> | <i>name</i>   | Name of the VLAN map.   |
|                           | <i>number</i>   | (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. |
| <b>Command Default</b>    | There are no VLAN map entries and no VLAN maps applied to a VLAN.   |   |
| <b>Command Modes</b>      | Global configuration (config)   |   |
| <b>Command History</b>    | <b>Release</b>  | <b>Modification</b>   |
|                           | Cisco IOS XE Everest 16.6.1   | This command was introduced.  |
| <b>Usage Guidelines</b>   | 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 <b>match</b> access-map configuration command to specify the access lists for IP or non-IP traffic to match and use the <b>action</b> command to set whether a match causes the packet to be forwarded or dropped.   |   |
|                           | In VLAN access-map configuration mode, these commands are available: <ul style="list-style-type: none"> <li>• <b>action</b>—Sets the action to be taken (forward or drop).</li> <li>• <b>default</b>—Sets a command to its defaults.</li> <li>• <b>exit</b>—Exits from VLAN access-map configuration mode.</li> <li>• <b>match</b>—Sets the values to match (IP address or MAC address).</li> <li>• <b>no</b>—Negates a command or set its defaults.</li> </ul> |   |
|                           | 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 <b>no vlan access-map</b> <i>name</i> [ <i>number</i> ] command with a sequence number to delete a single entry.  |   |
|                           | Use the <b>vlan filter</b> interface configuration command to apply a VLAN map to one or more VLANs.  |   |
| <b>Examples</b>           | 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> enable
Device# configure terminal
Device(config)# vlan access-map vac1
Device(config-access-map)# match ip address acl1
Device(config-access-map)# action forward
Device(config-access-map)# end
```

This example shows how to delete VLAN map vac1:

```
Device> enable
Device# configure terminal
Device(config)# no vlan access-map vac1
Device(config)# exit
```

# vlan dot1Q tag native

To enable dot1q (IEEE 802.1Q) tagging for a native VLAN on a trunk port, use the **vlan dot1Q tag native** command in global configuration mode.

To disable this function, use the **no** form of this command.

**vlan dot1Q tag native**  
**no vlan dot1Q tag native**

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

**Command Default** Disabled

**Command Modes** Global configuration (config)

| Command History | Release                      | Modification                 |
|-----------------|------------------------------|------------------------------|
|                 | Cisco IOS XE Everest 16.5.1a | This command was introduced. |

**Usage Guidelines** Typically, you configure 802.1Q trunks with a native VLAN ID which strips tagging from all packets on that VLAN.

To maintain the tagging on the native VLAN and drop untagged traffic, use the **vlan dot1q tag native** command. The device will tag the traffic received on the native VLAN and admit only 802.1Q-tagged frames, dropping any untagged traffic, including untagged traffic in the native VLAN.

Control traffic continues to be accepted as untagged on the native VLAN on a trunked port, even when the **vlan dot1q tag native** command is enabled.



**Note** If the **dot1q tag vlan native** command is configured at global level, dot1x reauthentication will fail on trunk ports.

This example shows how to enable dot1q (IEEE 802.1Q) tagging for native VLANs on all trunk ports on a device:

```
Device(config)# vlan dot1q tag native
Device(config)#
```

## Related Commands

| Command                           | Description  |
|-----------------------------------|--|
| <b>show vlan dot1q tag native</b> | Displays the status of tagging on the native VLAN. |

# vlan filter

To apply a VLAN map to one or more VLANs, use the **vlan filter** command in global configuration mode. Use the **no** form of this command to remove the map.

```
vlan filter mapname vlan-list {list | all}
no vlan filter mapname vlan-list {list | all}
```

|                           |  |   |
|---------------------------|--|---|
| <b>Syntax Description</b> | <i>mapname</i>   | Name of the VLAN map entry.   |
|                           | <b>vlan-list</b>   | Specifies which VLANs to apply the map to.  |
|                           | <i>list</i>  | 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. |
|                           | <b>all</b>   | Adds the map to all VLANs.  |
| <b>Command Default</b>    | There are no VLAN filters.   |   |
| <b>Command Modes</b>      | Global configuration (config)  |   |
| <b>Command History</b>    | <b>Release</b>   | <b>Modification</b>   |
|                           | Cisco IOS XE Everest 16.6.1  | This command was introduced.  |
| <b>Usage Guidelines</b>   | 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. |   |

## Examples

This example applies VLAN map entry map1 to VLANs 20 and 30:

```
Device> enable
Device# configure terminal
Device(config)# vlan filter map1 vlan-list 20, 30
Device(config)# exit
```

This example shows how to delete VLAN map entry mac1 from VLAN 20:

```
Device> enable
Device# configure terminal
Device(config)# no vlan filter map1 vlan-list 20
Device(config)# exit
```

You can verify your settings by entering the **show vlan filter** 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

|                                   |  |
|-----------------------------------|--|
| <i>group-name</i>                 | Name of the VLAN group. The group name may contain up to 32 characters and must begin with a letter.   |
| <b>vlan-list</b> <i>vlan-list</i> | Specifies one or more VLANs to be added to the VLAN group. The <i>vlan-list</i> 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 Modes

Global configuration (config)

## Command History

| Release                     | Modification                 |
|-----------------------------|------------------------------|
| Cisco IOS XE Everest 16.6.1 | 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.

## Examples

This example shows how to map VLANs 7 through 9 and 11 to a VLAN group:

```
Device> enable
Device# configure terminal
Device(config)# vlan group group1 vlan-list 7-9,11
Device(config)# exit
```

This example shows how to remove VLAN 7 from the VLAN group:

```
Device> enable
Device# configure terminal
Device(config)# no vlan group group1 vlan-list 7
Device(config)# exit
```