



# 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 authorization, on page 12](#)
- [aaa authorization network, on page 16](#)
- [aaa new-model, on page 17](#)
- [aaa policy interface-config allow-subinterface, on page 19](#)
- [access-session mac-move deny, on page 20](#)
- [access-session template monitor, on page 22](#)
- [action, on page 23](#)
- [authentication host-mode, on page 24](#)
- [authentication mac-move permit, on page 26](#)
- [authentication priority, on page 28](#)
- [authentication violation, on page 31](#)
- [cisp enable, on page 33](#)
- [clear errdisable interface vlan, on page 34](#)
- [clear mac address-table, on page 35](#)
- [confidentiality-offset, on page 37](#)
- [cts manual, on page 38](#)
- [cts role-based enforcement, on page 39](#)
- [cts role-based l2-vrf, on page 41](#)
- [cts role-based monitor, on page 43](#)
- [cts role-based permissions, on page 44](#)
- [delay-protection, on page 45](#)
- [deny \(MAC access-list configuration\), on page 46](#)
- [device-role \(IPv6 snooping\), on page 50](#)
- [device-role \(IPv6 nd inspection\), on page 51](#)
- [device-tracking policy, on page 52](#)
- [dot1x critical \(global configuration\), on page 54](#)
- [dot1x max-start, on page 55](#)
- [dot1x supplicant controlled transient, on page 56](#)
- [dot1x supplicant force-multicast, on page 57](#)

- dot1x test eapol-capable, on page 58
- dot1x test timeout, on page 59
- dot1x timeout, on page 60
- epm access-control open, on page 62
- include-icv-indicator, on page 63
- ip access-list role-based, on page 64
- ip admission, on page 65
- ip admission name, on page 66
- ip device tracking maximum, on page 68
- ip device tracking probe, on page 69
- ip dhcp snooping database, on page 70
- ip dhcp snooping information option format remote-id, on page 72
- ip dhcp snooping verify no-relay-agent-address, on page 73
- ip http access-class, on page 74
- ip radius source-interface, on page 76
- ip source binding, on page 78
- ip verify source, on page 79
- ipv6 access-list, on page 80
- ipv6 snooping policy, on page 82
- key chain macsec, on page 83
- key-server, on page 84
- limit address-count, on page 85
- mab request format attribute 32, on page 86
- macsec-cipher-suite, on page 88
- macsec network-link, on page 90
- match (access-map configuration), on page 91
- mka pre-shared-key, on page 93
- authentication logging verbose, on page 94
- dot1x logging verbose, on page 95
- mab logging verbose, on page 96
- permit (MAC access-list configuration), on page 97
- propagate sgt (cts manual), on page 101
- protocol (IPv6 snooping), on page 103
- radius server, on page 104
- sap mode-list (cts manual), on page 106
- security level (IPv6 snooping), on page 108
- security passthru, on page 109
- server-private (RADIUS), on page 110
- show aaa clients, on page 112
- show aaa command handler, on page 113
- **show aaa local**, on page 114
- show aaa servers, on page 115
- show aaa sessions, on page 116
- show authentication brief, on page 117
- show authentication history, on page 120
- show authentication sessions, on page 121

- [show cts interface](#), on page 124
- [show cts role-based permissions](#), on page 126
- [show cisp](#), on page 128
- [show dot1x](#), on page 130
- [show eap pac peer](#), on page 132
- [show ip dhcp snooping statistics](#), on page 133
- [show radius server-group](#), on page 136
- [show storm-control](#), on page 138
- [show vlan access-map](#), on page 140
- [show vlan filter](#), on page 141
- [show vlan group](#), on page 142
- [storm-control](#), on page 143
- [switchport port-security aging](#), on page 146
- [switchport port-security mac-address](#), on page 148
- [switchport port-security maximum](#), on page 150
- [switchport port-security violation](#), on page 152
- [tacacs server](#), on page 154
- [tracking \(IPv6 snooping\)](#), on page 155
- [trusted-port](#), on page 157
- [vlan access-map](#), on page 158
- [vlan dot1Q tag native](#), on page 160
- [vlan filter](#), on page 161
- [vlan group](#), on page 162

## 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 groupname</i>	At least one of the keywords described in <a href="#">Table 1: AAA accounting Methods, on page 5</a>

### Command Default

AAA accounting is disabled.

### Command Modes

Global configuration

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	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 [Table 1: AAA accounting Methods, on page 5](#), 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 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. For a list of supported RADIUS accounting attributes, refer to the appendix RADIUS Attributes in the *Cisco IOS Security Configuration Guide*. For a list of supported TACACS+ accounting AV pairs, refer to the appendix TACACS+ Attribute-Value Pairs in the *Cisco IOS Security Configuration Guide*.



---

**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(config)# aaa accounting commands 15 default stop-only group TACACS+
```

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(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+
```

## 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

<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>	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 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 accounting.
<b>tacacs+</b>	(Optional) Enables TACACS+ accounting.

### Command Default

AAA accounting is disabled.

### Command Modes

Global configuration

### Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	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(config)# aaa new-model  
Device(config)# aaa accounting dot1x default start-stop group radius
```



## aaa accounting identity

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

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

### Syntax Description

<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

### Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

### Usage Guidelines

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

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

```
Device# authentication display new-style
```

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

- (1) If you save the config in this mode, it will be written to NVRAM in NEW-style config, and if you subsequently reload the router without reverting to legacy config and saving that, you will no longer be able to revert.
- (2) In this and legacy mode, Webauth is not IPv6-capable. It will only become IPv6-capable once you have entered new-style config manually, or have reloaded with config saved in 'authentication display new' mode.

```
Device# configure terminal
```

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

## aaa authentication dot1x

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

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

<b>Syntax Description</b>	<b>default</b>	The default method when a user logs in. Use the listed authentication method that follows this argument.
	<i>method1</i>	Specifies the server authentication. Enter the <b>group radius</b> keywords to use the list of all RADIUS servers for authentication.
	<b>Note</b>	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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

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

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

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

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

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

## aaa authorization

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

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

```
aaa authorization { auth-proxy | cache | commands level | config-commands | configuration
| console | credential-download | exec | multicast | network | reverse-access | template }
{ default | list_name } [method1 [ method2 . . . ]]
```

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

### Syntax Description

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

---

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

---

**Command Default**

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

**Command Modes**

Global configuration

**Command History**

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

**Usage Guidelines**

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

**Note**

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

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

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

**Note**

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

This table describes the method keywords.

**Table 2: aaa authorization Methods**

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

Cisco IOS software supports the following methods for authorization:

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

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

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



---

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

---

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

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

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

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

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

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



---

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

---

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

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

# aaa authorization network

To configure the switch to use user-RADIUS authorization for all network-related service requests, such as IEEE 802.1x VLAN assignment, use the **aaa authorization network** command in global configuration mode. To disable RADIUS user authorization, use the **no** form of this command

**aaa authorization network default group radius**  
**no aaa authorization network default**

<b>Syntax Description</b>	<b>default group radius</b> Use the list of all RADIUS hosts in the server group as the default authorization list.	
<b>Command Default</b>	Authorization is disabled.	
<b>Command Modes</b>	Global configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

**Usage Guidelines** Use the **aaa authorization network default group radius** global configuration command to allow the switch to download IEEE 802.1x authorization parameters from the RADIUS servers in the default authorization list. The authorization parameters are used by features such as VLAN assignment to get parameters from the RADIUS servers.

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

This example shows how to configure the switch for user RADIUS authorization for all network-related service requests:

```
Device(config)# aaa authorization network default group radius
```



## 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 16.5.1a	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.

The following example shows this restriction:

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

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

### Examples

The following example initializes AAA:

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

**Related Commands**

<b>Command</b>	<b>Description</b>
<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.

# aaa policy interface-config allow-subinterface

To enable authentication, authorization, and accounting (AAA) Link Control Protocol (LCP) interface configuration policy parameters, issue the **aaa policy interface-config allow-subinterface** command in global configuration mode. To disable LCP interface configuration policy parameters, use the **no** form of this command.

```
aaa policy interface-config allow-subinterface
no aaa policy interface-config allow-subinterface
```

## Syntax Description

**interface-config** Specifies the LCP interface configuration policy parameters.

**allow-subinterface** Specifies not to create a full virtual access interface by default.

## Command Modes

Global configuration (config)

## Command History

Release	Modification
Cisco IOS XE 3.6.0E	This command was introduced.

## Usage Guidelines

Use the **interface-config** keyword to apply interface configuration mode commands on the virtual access interface associated with the session.

## Examples

The following example shows how to enable AAA LCP interface configuration policy parameters:

```
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa policy interface-config allow-subinterface
```

## Related Commands

Command	Description
<b>aaa new-model</b>	Enables the AAA access control model.

## access-session mac-move deny

To disable MAC move on a device, use the **access-session mac-move deny** global configuration command. To return to the default setting, use the **no** form of this command.

**access-session mac-move deny**  
**no access-session mac-move deny**

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

**Command Default** MAC move is enabled.

**Command Modes** Global configuration

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

**Usage Guidelines** The **no** form of this 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(config)# no access-session mac-move deny
```

### 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 for clients 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>Command</b>	<b>Description</b>
<b>authentication priority</b>	Adds an authentication method to the port-priority list.
<b>authentication timer</b>	Configures the timeout and reauthentication parameters for an 802.1x-enabled port.
<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>show authentication</b>	Displays information about authentication manager events on the switch.

# access-session template monitor

To set the access session template to monitor ports, use the **access-session template monitor** command in global configuration mode. To return to the default setting, use the **no** form of this command.

**access-session template monitor**

**no access-session template monitor**

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

**Command Default** This command is not configured.

**Command Modes** Global configuration (config)

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

**Usage Guidelines** The **access-session template monitor** command enables session monitoring to create sessions on all ports where authentication configurations are not present, and MAC addresses are known. These sessions have open access ports for traffic, multi-auth host mode to control the number of hosts on a port, and port-control set to auto for sessions to undergo authentication and authorization. The **access-session template monitor** command is enabled by default if the **device classifier** or **autoconf** command is enabled. Session monitoring can be disabled on a per port basis.

This command is available on devices that has Identity-Based Networking Services (IBNS). The equivalent command for **access-session template monitor** command in IBNS **new-style** mode is **access-session monitor**. To switch from IBNS legacy mode to new style mode, use the **authentication convert-to new-style** command.

## Examples

The following example shows how to set the access session template to monitor ports:

```
Device(config)# access-session template monitor
```

## Related Commands

Command	Description
<b>device classifier</b>	Creates a monitor session for all the MAC addresses learned in the system.
<b>authentication convert-to new-style</b>	Converts all the relevant authentication commands to their CPL control policy-equivalents.

# action

To set the action for the VLAN access map entry, use the **action** command in access-map configuration mode. To return to the default setting, use the **no** form of this command.

```
action {drop | forward}
no action
```

<b>Syntax Description</b>	<b>drop</b>	Drops the packet when the specified conditions are matched.
	<b>forward</b>	Forwards the packet when the specified conditions are matched.
<b>Command Default</b>	The default action is to forward packets.	
<b>Command Modes</b>	Access-map configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

**Usage Guidelines**

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

If the action is **drop**, you should define the access map, including configuring any access control list (ACL) names in match clauses, before applying the map to a VLAN, or all packets could be dropped.

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

The drop and forward parameters are not used in the **no** form of the command.

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

This example shows how to identify and apply a VLAN access map (vmap4) to VLANs 5 and 6 that causes the VLAN to forward an IP packet if the packet matches the conditions defined in access list a12:

```
Device(config)# vlan access-map vmap4
Device(config-access-map)# match ip address a12
Device(config-access-map)# action forward
Device(config-access-map)# exit
Device(config)# vlan filter vmap4 vlan-list 5-6
```

# 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		
<b>multi-auth</b>		Enables multiple-authorization mode (multi-auth mode) on the port.
<b>multi-domain</b>		Enables multiple-domain mode on the port.
<b>multi-host</b>		Enables multiple-host mode on the port.
<b>single-host</b>		Enables single-host mode on the port.

**Command Default** Single host mode is enabled.

**Command Modes** Interface configuration

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	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:

```
Device(config-if)# authentication host-mode multi-auth
```

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

```
Device(config-if)# authentication host-mode multi-domain
```

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



```
Device(config-if) # authentication host-mode multi-host
```

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

```
Device(config-if) # authentication host-mode single-host
```

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

# 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

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

**Usage Guidelines** This is a legacy command. The new command is **access-session mac-move deny**.

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(config)# authentication mac-move permit
```

## 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 fallback method for clients 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>	Enable or disables reauthentication on a port.

<b>Command</b>	<b>Description</b>
<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 an 802.1x-enabled port.
<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>show authentication</b>	Displays information about authentication manager events on the switch.

# 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}
```

<b>Syntax Description</b>	<p><b>dot1x</b> (Optional) Adds 802.1x to the order of authentication methods.</p> <hr/> <p><b>mab</b> (Optional) Adds MAC authentication bypass (MAB) to the order of authentication methods.</p> <hr/> <p><b>webauth</b> Adds web authentication to the order of authentication methods.</p>				
<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				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.5.1a</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.5.1a	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.5.1a	This command was introduced.				
<b>Usage Guidelines</b>	<p>Ordering sets the order of methods that the switch attempts when trying to authenticate a new device is connected to a port.</p> <p>When configuring multiple fallback methods on a port, set web authentication (webauth) last.</p> <p>Assigning priorities to different authentication methods allows a higher-priority method to interrupt an in-progress authentication method with a lower priority.</p>				
 <b>Note</b>	<p>If a client is already authenticated, it might be reauthenticated if an interruption from a higher-priority method occurs.</p> <hr/> <p>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 <b>dot1x</b>, <b>mab</b>, and <b>webauth</b> keywords to change this default order.</p> <p>This example shows how to set 802.1x as the first authentication method and web authentication as the second authentication method:</p> <pre>Device(config-if)# authentication priority dotx webauth</pre> <p>This example shows how to set MAB as the first authentication method and web authentication as the second authentication method:</p>				

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

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 unrecognized user credentials.
	<b>authentication event no-response action</b>	Specifies how the Auth Manager handles authentication failures as a result of a nonresponsive host.
	<b>authentication event server alive action reinitialize</b>	Reinitializes an authorized Auth Manager session when a previously unreachable authentication, authorization, 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 client on a port.
	<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 authorized ports.
	<b>authentication timer restart</b>	Specifies the period of time after which the Auth Manager attempts to authenticate an unauthorized port.
	<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.

Command	Description
<b>show authentication registrations</b>	Displays information about the authentication methods that are registered with the Auth Manager.
<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	Mode	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

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	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(config-if) # authentication violation shutdown
```

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(config-if) # authentication violation restrict
```

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

```
Device(config-if) # authentication violation protect
```

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(config-if) # authentication violation replace
```

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



# cisp enable

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

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

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

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

**Command Modes** Global configuration

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.
		This command was reintroduced. This command was not supported in and

**Usage Guidelines** The link between the authenticator and supplicant switch is a trunk. When you enable VTP on both switches, 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 switches, which can be caused by two VTP servers in the same domain.
- Both switches have different configuration revision numbers.

This example shows how to enable CISP:

```
Device(config)# cisp enable
```

Related Commands	Command	Description
	<b>dot1x credentials</b> <i>profile</i>	Configures a profile on a supplicant switch.
	<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 reenab a VLAN that was error-disabled, use the **clear errdisable interface** command in privileged EXEC mode.

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

Syntax Description		
	<i>interface-id</i>	Specifies an interface.
	<i>vlan list</i>	(Optional) Specifies a list of VLANs to be reenabled. If a VLAN list is not specified, then all VLANs are reenabled.

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

**Usage Guidelines** You can reenab 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.

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

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

Related Commands	Command	Description
	<b>errdisable detect cause</b>	Enables error-disabled detection for a specific cause or all causes.
	<b>errdisable recovery</b>	Configures the recovery mechanism variables.
	<b>show errdisable detect</b>	Displays error-disabled detection status.
	<b>show errdisable recovery</b>	Displays error-disabled recovery timer information.
	<b>show interfaces status err-disabled</b>	Displays interface status of a list of interfaces in error-disabled state.

## 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 physical port or port channel.
<b>vlan</b> <i>vlan-id</i>		(Optional) Deletes all dynamic MAC addresses for the specified VLAN. The range is 1 to 4094.
<b>move update</b>		Clears the MAC address table move-update counters.
<b>notification</b>		Clears the notifications in the history table and reset the counters.

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

**Command Modes** Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

**Usage Guidelines** You can verify that the information was deleted by entering the **show mac address-table** privileged EXEC command.

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

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

Related Commands	Command	Description
	<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 switch.

Command	Description
<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 switch.
<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 16.5.1a	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.

# cts manual

To manually enable an interface for Cisco TrustSec Security (CTS), use the **cts manual** command in interface configuration mode.

## cts manual

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

**Command Default** Disabled

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

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was modified with additional options.
	Cisco IOS XE 3.7E	This command was introduced.

**Usage Guidelines** Use the **cts manual** command to enter the TrustSec manual interface configuration in which policies and the Security Association Protocol (SAP) are configured on the link.

When **cts manual** command is configured, 802.1X authentication is not performed on the link. Use the **policy** subcommand to define and apply policies on the link. By default no policy is applied. To configure MACsec link-to-link encryption, the SAP negotiation parameters must be defined. By default SAP is not enabled. The same SAP Pairwise master key (PMK) should be configured on both sides of the link (that is, a shared secret)

## Examples

The following example shows how to enter the Cisco TrustSec manual mode:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet 0
Switch(config-if)# cts manual
Switch(config-if-cts-manual)#
```

The following example shows how to remove the CTS manual configuration from an interface:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet 0
Switch(config-if)# no cts manual
```

Related Commands	Command	Description
	<b>propagate sgt (cts manual)</b>	Enables Security Group Tag (SGT) propagation at Layer 2 on Cisco TrustSec Security (CTS) interfaces.
	<b>sap mode-list (cts manual)</b>	Manually specifies the PMK and the SAP authentication and encryption modes to negotiate MACsec link encryption between two interfaces.
	<b>show cts interface</b>	Displays Cisco TrustSec interface configuration statistics.

## cts role-based enforcement

To enable Cisco TrustSec role-based (security group) access control enforcement, use the **cts role-based enforcement** command in global configuration mode. To disable the configuration, use the **no** form of this command.

```
cts role-based enforcement [{logging-interval interval | vlan-list {all | vlan-ID [{,}] [{-}]}}]
no cts role-based enforcement [{logging-interval interval | vlan-list {all | vlan-ID [{,}] [{-}]}}]
```

### Syntax Description

<b>logging-interval</b> <i>interval</i>	(Optional) Configures a logging interval for a security group access control list (SGACL). Valid values for the <i>interval</i> argument are from 5 to 86400 seconds. The default is 300 seconds
<b>vlan-list</b>	(Optional) Configures VLANs on which role-based ACLs are enforced.
<b>all</b>	(Optional) Specifies all VLANs.
<i>vlan-ID</i>	(Optional) VLAN ID. Valid values are from 1 to 4094.
,	(Optional) Specifies another VLAN separated by a comma.
-	(Optional) Specifies a range of VLANs separated by a hyphen.

### Command Default

Role-based access control is not enforced.

### Command Modes

Global configuration (config)

### Command History

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

### Usage Guidelines



**Note** RBACL and SGACL are used interchangeably.

Use the **cts role-based enforcement** command to globally enable or disable SGACL enforcement for Cisco TrustSec-enabled interfaces in the system.

The default interval after which log for a given flow is printed is 300 seconds. Use the **logging-interval** keyword to change the default interval. Logging is only triggered when the Cisco ACE Application Control Engine has the **logging** keyword.

SGACL enforcement is not enabled by default on VLANs. Use the **cts role-based enforcement vlan-list** command to enable or disable SGACL enforcement for Layer 2 switched packets and for Layer 3 switched packets on an switched virtual interface (SVI).

The *vlan-ID* argument can be a single VLAN ID, a list of VLAN IDs, or VLAN ID ranges.

When a VLAN in which a SGACL is enforced has an active SVI, the SGACL is enforced for both Layer 2 and Layer 3 switched packets within that VLAN. Without an SVI, the SGACL is enforced only for Layer 2 switched packets, because no Layer 3 switching is possible within a VLAN without an SVI.

The following example shows configure an SGACL logging interval:

```
Switch(config)# cts role-based enforcement logging-interval 90
Switch(config)# logging rate-limit

May 27 10:19:21.509: %RBM-6-SGACLHIT:
ingress_interface='GigabitEthernet1/0/2' sgacl_name='sgacl2' action='Deny'
protocol='icmp' src-ip='16.16.1.3' src-port='8' dest-ip='17.17.1.2' dest-port='0'
sgt='101' dgt='202' logging_interval_hits='5'
```

#### Related Commands

Command	Description
<b>logging rate-limit</b>	Limits the rate of messages logged per second.
<b>show cts role-based permissions</b>	Displays the SGACL permission list.



## cts role-based l2-vrf

To select a virtual routing and forwarding (VRF) instance for Layer 2 VLANs, use the **cts role-based l2-vrf** command in global configuration mode. To remove the configuration, use the **no** form of this command.

```
cts role-based l2-vrf vrf-name vlan-list {all vlan-ID} [{,}] [{}-]
no cts role-based l2-vrf vrf-name vlan-list {all vlan-ID} [{,}] [{}-]
```

### Syntax Description

<i>vrf-name</i>	Name of the VRF instance.
<b>vlan-list</b>	Specifies the list of VLANs to be assigned to a VRF instance.
<b>all</b>	Specifies all VLANs.
<i>vlan-ID</i>	VLAN ID. Valid values are from 1 to 4094.
,	(Optional) Specifies another VLAN separated by a comma.
-	(Optional) Specifies a range of VLANs separated by a hyphen.

### Command Default

VRF instances are not selected.

### Command Modes

Global configuration (config)

### Command History

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

### Usage Guidelines

The *vlan-list* argument can be a single VLAN ID, a list of comma-separated VLAN IDs, or hyphen-separated VLAN ID ranges.

The **all** keyword is equivalent to the full range of VLANs supported by the network device. The **all** keyword is not preserved in the nonvolatile generation (NVGEN) process.

If the **cts role-based l2-vrf** command is issued more than once for the same VRF, each successive command entered adds the VLAN IDs to the specified VRF.

The VRF assignments configured by the **cts role-based l2-vrf** command are active as long as a VLAN remains a Layer 2 VLAN. The IP-SGT bindings learned while a VRF assignment is active are also added to the Forwarding Information Base (FIB) table associated with the VRF and the IP protocol version. If an Switched Virtual Interface (SVI) becomes active for a VLAN, the VRF-to-VLAN assignment becomes inactive and all bindings learned on the VLAN are moved to the FIB table associated with the VRF of the SVI.

Use the **interface vlan** command to configure an SVI interface, and the **vrf forwarding** command to associate a VRF instance to the interface.

The VRF-to-VLAN assignment is retained even when the assignment becomes inactive. It is reactivated when the SVI is removed or when the SVI IP address is changed. When reactivated, the IP-SGT bindings are moved back from the FIB table associated with the VRF of the SVI to the FIB table associated with the VRF assigned by the **cts role-based l2-vrf** command.

The following example shows how to select a list of VLANs to be assigned to a VRF instance:

```
Switch(config)# cts role-based l2-vrf vrf1 vlan-list 20
```

The following example shows how to configure an SVI interface and associate a VRF instance:

```
Switch(config)# interface vlan 101  
Switch(config-if)# vrf forwarding vrf1
```

**Related Commands**

Command	Description
<b>interface vlan</b>	Configures a VLAN interface.
<b>vrf forwarding</b>	Associates a VRF instance or a virtual network with an interface or subinterface.
<b>show cts role-based permissions</b>	Displays the SGACL permission list.

## cts role-based monitor

To enable role-based (security-group) access list monitoring, use the **cts role-based monitor** command in global configuration mode. To remove role-based access list monitoring, use the **no** form of this command.

```
cts role-based monitor {all | permissions | {default | from {sgt | unknown}} to {sgt | unknown}
[{{ipv4}}]}
no cts role-based monitor {all | permissions | {default | from {sgt | unknown}} to {sgt | unknown}
[{{ipv4}}]}
```

### Syntax Description

<b>all</b>	Monitors permissions for all source tags to all destination tags.
<b>permissions</b>	Monitors permissions from a source tags to a destination tags.
<b>default</b>	Monitors the default permission list.
<b>from</b>	Specifies the source group tag for filtered traffic.
<i>sgt</i>	Security Group Tag (SGT). Valid values are from 2 to 65519.
<b>unknown</b>	Specifies an unknown source or destination group tag (DST).
<b>ipv4</b>	(Optional) Specifies the IPv4 protocol.

### Command Default

Role-based access control monitoring is not enabled.

### Command Modes

Global configuration (config)

### Command History

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

### Usage Guidelines

Use the **cts role-based monitor all** command to enable the global monitor mode. If the **cts role-based monitor all** command is configured, the output of the **show cts role-based permissions** command displays monitor mode for all configured policies as true.

The following examples shows how to configure SGACL monitor from a source tag to a destination tag:

```
Switch(config)# cts role-based monitor permissions from 10 to 11
```

### Related Commands

Command	Description
<b>show cts role-based permissions</b>	Displays the SGACL permission list.

## cts role-based permissions

To enable permissions from a source group to a destination group, use the **cts role-based permissions** command in global configuration mode. To remove the permissions, use the **no** form of this command.

```
cts role-based permissions {default ipv4 | from {sgt | unknown} to {sgt | unknown} {ipv4}
{rbacl-name [{rbacl-name....}]}}
no cts role-based permissions {default [{ipv4}] | from {sgt | unknown} to {sgt
| unknown} [{ipv4}]}
```

### Syntax Description

<b>default</b>	Specifies the default permissions list. Every cell (an SGT pair) for which, security group access control list (SGACL) permission is not configured statically or dynamically falls under the default category.
<b>ipv4</b>	Specifies the IPv4 protocol.
<b>from</b>	Specifies the source group tag of the filtered traffic.
<i>sgt</i>	Security Group Tag (SGT). Valid values are from 2 to 65519.
<b>unknown</b>	Specifies an unknown source or destination group tag.
<i>rbacl-name</i>	Role-based access control list (RBACL) or SGACL name. Up to 16 SGACLs can be specified in the configuration.

### Command Default

Permissions from a source group to a destination group is not enabled.

### Command Modes

Global configuration (config)

### Command History

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

### Usage Guidelines

Use the **cts role-based permissions** command to define, replace, or delete the list of SGACLs for a given source group tag (SGT), destination group tag (DGT) pair. This policy is in effect as long as there is no dynamic policy for the same DGT or SGT.

The **cts role-based permissions default** command defines, replaces, or deletes the list of SGACLs of the default policy as long as there is no dynamic policy for the same DGT.

The following example shows how to enable permissions for a destination group:

```
Switch(config)# cts role-based permissions from 6 to 6 mon_2
```

### Related Commands

Command	Description
<b>show cts role-based permissions</b>	Displays the SGACL permission list.

## 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 16.5.1a	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** MAC access-list configuration command on the switch stack or on a standalone switch. 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 | larc-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 | larc-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 the source address for a packet matches 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>	Defines a destination MAC address and optional subnet mask. If the destination address for a packet matches the defined address, non-IP traffic to that address is denied.
<i>type mask</i>	(Optional) Specifies the EtherType number of a packet with Ethernet II or SNAP encapsulation to identify the protocol of the packet.  The type is 0 to 65535, specified in hexadecimal.  The mask is a mask of don't care bits applied to the EtherType before testing for a match.
<b>aarp</b>	(Optional) Specifies EtherType AppleTalk Address Resolution Protocol that maps a data-link address 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 (DEC) spanning tree.
<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-LAVR-SCA.
<b>lsap</b> <i>lsap-number mask</i>	(Optional) Specifies the LSAP number (0 to 65535) of a packet with 802.2 encapsulation to identify the protocol of the packet.  <i>mask</i> is a mask of don't care bits applied to the LSAP number before testing for a match.
<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 (NetBIOS).
<b>vines-echo</b>	(Optional) Specifies EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems.
<b>vines-ip</b>	(Optional) Specifies EtherType VINES IP.
<b>xns-idp</b>	(Optional) Specifies EtherType Xerox Network Systems (XNS) protocol suite (0 to 65535), an arbitrary EtherType in decimal, hexadecimal, or octal.
<b>cos</b> <i>cos</i>	(Optional) Specifies a class of service (CoS) number from 0 to 7 to set priority. Filtering on CoS can be performed only in hardware. A warning message reminds the user if the <b>cos</b> option 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 configuration

**Command History**

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

**Usage Guidelines**

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 **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 terminology are listed in the table.

**Table 3: IPX Filtering Criteria**

IPX Encapsulation Type		Filter Criterion
Cisco IOS 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(config-ext-macl)# deny any host 00c0.00a0.03fa netbios.
```

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

```
Device(config-ext-macl)# no deny any 00c0.00a0.03fa 0000.0000.0000 netbios.
```

This example denies all packets with EtherType 0x4321:

```
Device(config-ext-macl)# deny any any 0x4321 0
```

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 for non-IP traffic.
<b>permit</b>	Permits from the MAC access-list configuration. Permits non-IP traffic to be forwarded if conditions are matched.



Command	Description
show access-lists	Displays access control lists configured on a switch.

## device-role (IPv6 snooping)

To specify the role of the device attached to the port, use the **device-role** command in IPv6 snooping configuration mode.

**device-role** { **node** | **switch** }

<b>Syntax Description</b>	<b>node</b> Sets the role of the attached device to node.
	<b>switch</b> Sets the role of the attached device to switch.

**Command Default** The device role is node.

**Command Modes** IPv6 snooping configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

**Usage Guidelines** The **device-role** command specifies the role of the device attached to the port. By default, the device role is node.

The **switch** keyword indicates that the remote device is a switch and that the local switch is now operating in multiswitch mode; binding entries learned from the port will be marked with trunk\_port preference level. If the port is configured as a trust-port, binding entries will be marked with trunk\_trusted\_port preference level.

This example shows how to define an IPv6 snooping policy name as policy1, place the device in IPv6 snooping configuration mode, and configure the device as the node:

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# device-role node
```

## device-role (IPv6 nd inspection)

To specify the role of the device attached to the port, use the **device-role** command in neighbor discovery (ND) inspection policy configuration mode.

```
device-role { host | 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	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Everest 16.5.1a	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 host, and therefore all the inbound router advertisement and redirect messages are blocked.

The **switch** keyword indicates that the remote device is a switch and that the local switch is now operating in multiswitch mode; binding entries learned from the port will be marked with trunk\_port preference level. If the port is configured as a trust-port, binding entries will be marked with trunk\_trusted\_port preference level.

The following example defines a Neighbor Discovery Protocol (NDP) policy name as policy1, places the device in ND inspection policy configuration mode, and configures the device as the host:

```
Device(config)# ipv6 nd inspection policy policy1
Device(config-nd-inspection)# device-role host
```

# device-tracking 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				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td></td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification		This command was introduced.
Release	Modification				
	This command was introduced.				

**Usage Guidelines** Use the SISF-based **device-tracking policy** command to create a device tracking policy. When the **device-tracking policy** command is enabled, the configuration mode changes to device-tracking configuration mode. In this mode, the administrator can configure the following first-hop security commands:

- (Optional) **device-role** {**node** | **switch**}—Specifies the role of the device attached to the port. Default is **node**.
- (Optional) **limit address-count** *value*—Limits the number of addresses allowed per target.
- (Optional) **no**—Negates a command or sets it to defaults.
- (Optional) **destination-glean** {**recovery** | **log-only**} [**dhcp**]}—Enables binding table recovery by data traffic source address gleaning.
- (Optional) **data-glean** {**recovery** | **log-only**} [**dhcp** | **ndp**]}—Enables binding table recovery using source or data address gleaning.
- (Optional) **security-level** {**glean** | **guard** | **inspect**}—Specifies the level of security enforced by the feature. Default is **guard**.
  - glean**—Gleans addresses from messages and populates the binding table without any verification.
  - guard**—Gleans addresses and inspects messages. In addition, it rejects RA and DHCP server messages. This is the default option.
  - inspect**—Gleans addresses, validates messages for consistency and conformance, and enforces address ownership.
- (Optional) **tracking** {**disable** | **enable**}—Specifies a tracking option.
- (Optional) **trusted-port**—Sets up a trusted port. It disables the guard on applicable targets. Bindings learned through a trusted port have preference over bindings learned through any other port. A trusted port is given preference in case of a collision while making an entry in the table.

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

```
Device(config)# device-tracking policy policy1  
Device(config-device-tracking)# trusted-port
```

## 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

<b>Syntax Description</b>	<b>eapol</b> Specifies that the switch send an EAPOL-Success message when the switch successfully authenticates the critical port.				
<b>Command Default</b>	<b>eapol</b> is disabled				
<b>Command Modes</b>	Global configuration				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.5.1a</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.5.1a	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.5.1a	This command was introduced.				

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

```
Device(config)# dot1x critical eapol
```

## dot1x max-start

To set the maximum number of Extensible Authentication Protocol over LAN (EAPOL) start frames that a supplicant sends (assuming that no response is received) to the client before concluding that the other end is 802.1X unaware, use the **dot1x max-start** command in interface configuration mode. To remove the maximum number-of-times setting, use the **no** form of this command.

```
dot1x max-start number
no dot1x max-start
```

### Syntax Description

*number* Maximum number of times that the router sends an EAPOL start frame. The value is from 1 to 10. The default is 3.

### Command Default

The default maximum number setting is 3.

### Command Modes

Interface configuration

### Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

### Usage Guidelines

You must enter the **switchport mode access** interface configuration command on a switch port before entering this command.

The following example shows that the maximum number of EAPOL Start requests has been set to 5:

```
Device(config)# interface g1/0/3
Device(config-if)# dot1x max-start 5
```

## 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

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.
		This command was reintroduced. This command was not supported in and

**Usage Guidelines** In the default state, when you connect a supplicant switch 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. Beginning with Cisco IOS Release 15.0(1)SE, you can control traffic exiting the supplicant port during the authentication period. Entering the **dot1x supplicant controlled transient** global configuration 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** global configuration command opens the supplicant port during the authentication period. This is the default behavior.

We strongly recommend using the **dot1x supplicant controlled transient** command on a supplicant switch 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 switch during authentication:

```
Device(config)# dot1x supplicant controlled transient
```



## 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 switch 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

### Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.
	This command was reintroduced. This command was not supported in and

### Usage Guidelines

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

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

```
Device(config)# dot1x supplicant force-multicast
```

### Related Commands

Command	Description
<b>cisp enable</b>	Enable Client Information Signalling Protocol (CISP) on a switch so that it acts as an authenticator to a supplicant switch.
<b>dot1x credentials</b>	Configure the 802.1x supplicant credentials on the port.
<b>dot1x pae supplicant</b>	Configure an interface to act only as a supplicant.

## 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 on the switch stack or on a standalone switch.

**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 16.5.1a	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# 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 wait for EAPOL response to an IEEE 802.1x 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 on the switch stack or on a standalone switch.

**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.
<b>Command Default</b>	The default setting is 10 seconds.	
<b>Command Modes</b>	Global configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Everest 16.5.1a	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# dot1x test timeout 27
```

You can verify the timeout configuration status by entering the **show run** privileged EXEC command.

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>dot1x test eapol-capable</b> [ <i>interface 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).  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).  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.  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 switch 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.  The range is from 1 to 65535. The default is 30.  In Cisco IOS Release 15.2(5)E, this command is only available in the supplicant mode. If the command is applied in any other mode, the command misses from the configuration.

<b>supp-timeout</b> <i>seconds</i>	Sets the authenticator-to-supplicant retransmission time for all EAP messages other than EAP Request ID.  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.  <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>

**Command Default** Periodic reauthentication and periodic rate-limiting are done.

**Command Modes** Interface configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Everest 16.5.1a	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 switch only if you have enabled periodic re-authentication by using the **dot1x reauthentication** interface configuration command.

During the quiet period, the switch 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 switch 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(config)# configure terminal
Device(config)# interface g1/0/3
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
```

# 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

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	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** privileged EXEC command.

This example shows how to configure an open directive.

```
Device(config)# epm access-control open
```

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)

Release	Modification
Cisco IOS XE Everest 16.5.1a	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 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 Denali 16.3.1	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:

```
Switch(config)# ip access-list role-based rbacl1
Switch(config-rb-acl)# permit ip log
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<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. You can also use this command in fallback-profile configuration mode. To disable web authentication, use the **no** form of this command.

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

---

**Syntax Description**      *rule* IP admission rule name.

---



---

**Command Default**      Web authentication is disabled.

---



---

**Command Modes**      Interface configuration  
 Fallback-profile configuration

---



---

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

---



---

**Usage Guidelines**      The **ip admission** command applies a web authentication rule to a switch port.

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

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

This example shows how to apply a web authentication rule to a fallback profile for use on an IEEE 802.1x enabled switch port.

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

## ip 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.

### Command Default

Web authentication is disabled.

### Command Modes

Global configuration

### Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	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# 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# 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 device tracking maximum

To configure IP device tracking parameters on a Layer 2 access port, use the **ip device tracking maximum** command in interface configuration mode. To remove the maximum value, use the **no** form of the command.

**ip device tracking maximum** *number*  
**no ip device tracking maximum**

<b>Syntax Description</b>	<i>number</i> Number of bindings created in the IP device tracking table for a port. The range is 0 (disabled) to 65535.				
<b>Command Default</b>	None				
<b>Command Modes</b>	Interface configuration mode				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.5.1a</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.5.1a	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.5.1a	This command was introduced.				

**Usage Guidelines**

To remove the maximum value, use the **no ip device tracking maximum** command.

To disable IP device tracking, use the **ip device tracking maximum 0** command.



**Note** This command enables IPDT wherever its configured

## Examples

This example shows how to configure IP device tracking parameters on a Layer 2 access port:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# ip device tracking
Device(config)# interface gigabitethernet1/0/3
Device(config-if)# switchport mode access
Device(config-if)# switchport access vlan 1
Device(config-if)# ip device tracking maximum 5
Device(config-if)# switchport port-security
Device(config-if)# switchport port-security maximum 5
Device(config-if)# end
```

## ip device tracking probe

To configure the IP device tracking table for Address Resolution Protocol (ARP) probes, use the **ip device tracking probe** command in global configuration mode. To disable ARP probes, use the **no** form of this command.

```
ip device tracking probe {count number | delay seconds | interval seconds | use-svi address}
no ip device tracking probe {count number | delay seconds | interval seconds | use-svi address}
```

Syntax Description	
<b>count</b> <i>number</i>	Sets the number of times that the device sends the ARP probe. The range is from 1 to 255.
<b>delay</b> <i>seconds</i>	Sets the number of seconds that the device waits before sending the ARP probe. The range is from 1 to 120.
<b>interval</b> <i>seconds</i>	Sets the number of seconds that the device waits for a response before resending the ARP probe. The range is from 30 to 1814400 seconds.
<b>use-svi</b>	Uses the switch virtual interface (SVI) IP address as source of ARP probes.

Command Default	
	The count number is 3.
	There is no delay.
	The interval is 30 seconds.
	The ARP probe default source IP address is the Layer 3 interface and 0.0.0.0 for switchports.

Command Modes	
	Global configuration

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

Usage Guidelines	
	Use the <b>use-svi</b> keyword to configure the IP device tracking table to use the SVI IP address for ARP probes in cases when the default source IP address 0.0.0.0 for switch ports is used and the ARP probes drop.

Examples	
	This example shows how to set SVI as the source for ARP probes:

```
Device(config)# ip device tracking probe use-svi
```

## 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 ]
```

### Syntax Description

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

---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Everest 16.5.1a	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(config)# ip dhcp snooping database tftp://10.90.90.90/snooping-rp2
```


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

```
Device(config)# ip dhcp snooping database write-delay 15
```

## 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 switch 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}
```

<b>Syntax Description</b>	<b>hostname</b> Specify the switch hostname as the remote ID.				
	<b>string string</b> Specify a remote ID, using from 1 to 63 ASCII characters (no spaces).				
<b>Command Default</b>	The switch MAC address is the remote ID.				
<b>Command Modes</b>	Global configuration				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.5.1a</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.5.1a	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.5.1a	This command was introduced.				
<b>Usage Guidelines</b>	<p>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.</p> <p>When the option-82 feature is enabled, the default remote-ID suboption is the switch MAC address. This command allows you to configure either the switch hostname or a string of up to 63 ASCII characters (but no spaces) to be the remote ID.</p>				
 <b>Note</b>	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(config)# ip dhcp snooping information option format remote-id hostname
```



## 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

### Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	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 reenables verification.

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

```
Device(config)# no ip dhcp snooping verify no-relay-agent-address
```

## 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.



**Note** The existing **ip http access-class** *access-list-number* command is currently supported, but is going to be deprecated. Use the **ip http access-class ipv4** { *access-list-number* | *access-list-name* } and **ip http access-class ipv6** *access-list-name* instead.

```
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

<b>ipv4</b>	Specifies the IPv4 access list to restrict access to the secure HTTP server.
<b>ipv6</b>	Specifies the IPv6 access list to restrict access to the secure HTTP server.
<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.
<i>access-list-name</i>	Name of a standard IPv4 access list, as configured by the <b>ip access-list</b> command.

### Command Default

No access list is applied to the HTTP server.

### Command Modes

Global configuration (config)

### Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was modified. The <b>ipv4</b> and <b>ipv6</b> keyword were added.
Cisco IOS XE Release 3.3SE	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(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
```

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

```
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
```

#### 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**

Syntax Description	
<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)

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	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 vrf1
```

## 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.	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Everest 16.5.1a	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# configure terminal
Deviceconfig) ip source binding 0100.0230.0002 vlan 11 10.0.0.4 interface gigabitethernet1/0/1
```

## 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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Everest 16.5.1a	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(config)# interface gigabitethernet1/0/1
Device(config-if)# ip verify source
```

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

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

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

## 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.  <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.  <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

### Command History

Release	Modification
	This command was reintroduced. This command was not supported in and

### Usage Guidelines

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



### Note

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

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

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



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

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

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

## Examples

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

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

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

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

# ipv6 snooping policy



**Note** All existing IPv6 Snooping commands (prior to ) now have corresponding SISF-based device-tracking commands that allow you to apply your configuration to both IPv4 and IPv6 address families. For more information, see [device-tracking policy](#)

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

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

**Syntax Description** *snooping-policy* User-defined name of the snooping policy. The policy name can be a symbolic string (such as Engineering) or an integer (such as 0).

**Command Default** An IPv6 snooping policy is not configured.

**Command Modes** Global configuration

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

**Usage Guidelines** Use the **ipv6 snooping policy** command to create an IPv6 snooping policy. When the **ipv6 snooping policy** command is enabled, the configuration mode changes to IPv6 snooping configuration mode. In this mode, the administrator can configure the following IPv6 first-hop security commands:

- The **device-role** command specifies the role of the device attached to the port.
- The **limit address-count** *maximum* command limits the number of IPv6 addresses allowed to be used on the port.
- The **protocol** command specifies that addresses should be gleaned with Dynamic Host Configuration Protocol (DHCP) or Neighbor Discovery Protocol (NDP).
- The **security-level** command specifies the level of security enforced.
- The **tracking** command overrides the default tracking policy on a port.
- The **trusted-port** command configures a port to become a trusted port; that is, limited or no verification is performed when messages are received.

This example shows how to configure an IPv6 snooping policy:

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)#
```

# 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** {**description** | **key** | **exit**}

Syntax Description	
<b>name</b>	Name of a key chain to be used to get keys.
<b>description</b>	Provides description of the MACsec key chain.
<b>key</b>	Configure a MACsec key.
<b>exit</b>	Exits from the MACsec key-chain configuration mode.
<b>no</b>	Negates the command or sets the default values.

**Command Default** key chain macsec is disabled.

**Command Modes** Global configuration

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

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

```
Switch#configure terminal
Switch(config)#key chain kcl macsec
Switch(config-keychain-macsec)#key 1000
Switch(config-keychain-macsec)#cryptographic-algorithm aes-128-cmac
Switch(config-keychain-macsec-key)# key-string fb63e0269e2768c49bab8ee9a5c2258f
Switch(config-keychain-macsec-key)#end
Switch#
```

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

```
Switch#configure terminal
Switch(config)#key chain kcl macsec
Switch(config-keychain-macsec)#key 2000
Switch(config-keychain-macsec)#cryptographic-algorithm aes-256-cmac
Switch(config-keychain-macsec-key)# key-string
c865632acb269022447c417504a1bf5db1c296449b52627ba01f2ba2574c2878
Switch(config-keychain-macsec-key)#end
Switch#
```

# 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**

<b>Syntax Description</b>	<b>priority</b> <i>value</i>	Specifies the priority value of the MKA key-server.
---------------------------	------------------------------	---

<b>Command Default</b>	MKA key-server is disabled.
------------------------	-----------------------------

<b>Command Modes</b>	MKA-policy configuration (config-mka-policy)
----------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Everest 16.5.1a	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**

### Syntax Description

*maximum* The number of addresses allowed on the port. The range is from 1 to 10000.

### Command Default

The default is no limit.

### Command Modes

ND inspection policy configuration

IPv6 snooping configuration

### Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

### Usage Guidelines

The **limit address-count** 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.

This example shows how to define an NDP policy name as policy1, place the switch in NDP inspection policy configuration mode, and limit the number of IPv6 addresses allowed on the port to 25:

```
Device(config)# ipv6 nd inspection policy policy1
Device(config-nd-inspection)# limit address-count 25
```

This example shows how to define an IPv6 snooping policy name as policy1, place the switch in IPv6 snooping policy configuration mode, and limit the number of IPv6 addresses allowed on the port to 25:

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# limit address-count 25
```

## mab request format attribute 32

To enable VLAN ID-based MAC authentication on a switch, 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

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	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 switch:

```
Device(config)# mab request format attribute 32 vlan access-vlan
```

### 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 for clients 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>Command</b>	<b>Description</b>
<b>authentication timer</b>	Configures the timeout and reauthentication parameters for an 802.1x-enabled port.
<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 switch.

# 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 | gcm-aes-xpn-128 | gcm-aes-xpn-256}
no macsec-cipher-suite {gcm-aes-128 | gcm-aes-256 | gcm-aes-xpn-128 | gcm-aes-xpn-256}
```

## Syntax Description

<b>gcm-aes-128</b>	Configures cipher suite for deriving SAK with 128-bit encryption.
<b>gcm-aes-256</b>	Configures cipher suite for deriving SAK with 256-bit encryption.
<b>gcm-aes-xpn-128</b>	Configures cipher suite for deriving SAK with 128-bit encryption for Extended Packet Numbering (XPN).
<b>gcm-aes-xpn-256</b>	Configures cipher suite for deriving SAK with 256-bit encryption for XPN.

## Command Default

GCM-AES-128 encryption is enabled.

## Command Modes

MKA-policy configuration (config-mka-policy)

## Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	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>Command</b>	<b>Description</b>
<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.

## macsec network-link

To enable MKA MACsec configuration on the uplink interfaces, use the **macsec network-link** command on the interface. To disable it, use the **no** form of this command.

### macsec network-link

#### Syntax Description

**macsec network-link** Enables MKA MACsec configuration on device interfaces using EAP-TLS authentication protocol.

#### Command Default

macsec network-link is disabled.

#### Command Modes

Interface configuration

#### Command History

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

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

```
Switch#configure terminal
Switch(config)# int G1/0/20
Switch(config-if)# macsec network-link
Switch(config-if)# end
Switch#
```

## match (access-map configuration)

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

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

Syntax Description	
<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

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

**Usage Guidelines** You enter access-map configuration mode by using the **vlan access-map** global configuration command. You must enter one access list name or number; others are optional. You can match packets against one or more access lists. Matching any of the lists counts as a match of the entry.

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

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

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

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

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

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

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

## mka pre-shared-key

To configure 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 global configuration mode. To disable it, use the **no** form of this command.

**mka pre-shared-key key-chain** *key-chain-name*

<b>Syntax Description</b>	<b>mka pre-shared-key key-chain</b> Enables MACsec MKA configuration on device interfaces using a PSK.				
<b>Command Default</b>	mka pre-shared-key is disabled.				
<b>Command Modes</b>	Interface configuration				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Denali 16.3.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Denali 16.3.1	This command was introduced.
Release	Modification				
Cisco IOS XE Denali 16.3.1	This command was introduced.				

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

```
Switch#
Switch(config)# int G1/0/20
Switch(config-if)# mka pre-shared-key key-chain kc1
Switch(config-if)# end
Switch#
```

# 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 16.5.1a	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(config)# authentication logging verbose
```

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 802.1x system messages.
<b>mab logging verbose</b>	Filters details from MAC authentication bypass (MAB) system messages.

# dot1x logging verbose

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

```
dot1x logging verbose
no dot1x 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 16.5.1a	This command was introduced.

**Usage Guidelines** This command filters details, such as anticipated success, from 802.1x system messages. Failure messages are not filtered.

To filter verbose 802.1x system messages:

```
Device(config)# dot1x logging verbose
```

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 802.1x system messages.
	<b>mab logging verbose</b>	Filters details from MAC authentication bypass (MAB) system messages.

# mab logging verbose

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

**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 16.5.1a	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(config)# mab logging verbose
```

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 802.1x system messages.
<b>mab logging verbose</b>	Filters details from MAC authentication bypass (MAB) system messages.



## permit (MAC access-list configuration)

To allow non-IP traffic to be forwarded if the conditions are matched, use the **permit** MAC access-list configuration command on the switch stack or on a standalone switch. 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 | larc-sca | lsap/sap 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 | larc-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 source address for a packet matches 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 destination address for a packet matches the defined address, non-IP traffic to that address is denied.
<i>type mask</i>	(Optional) Specifies the EtherType number of a packet with Ethernet II or SNAP encapsulation 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 before testing for a match.</li> </ul>
<b>aarp</b>	(Optional) Specifies EtherType AppleTalk Address Resolution Protocol that maps a data-link address 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 (DEC) spanning tree.
<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 a packet with 802.2 encapsulation to identify the protocol of the packet.  The <i>mask</i> is a mask of don't care bits applied to the LSAP number before testing for a match.
<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 (NetBIOS).
<b>vines-echo</b>	(Optional) Specifies EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems.
<b>vines-ip</b>	(Optional) Specifies EtherType VINES IP.
<b>xns-idp</b>	(Optional) Specifies EtherType Xerox Network Systems (XNS) protocol suite.
<b>cos</b> <i>cos</i>	(Optional) Specifies an arbitrary class of service (CoS) number from 0 to 7 to set priority. Filtering on CoS can be performed only in hardware. A warning message appears if the <b>cos</b> option 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 configuration

**Command History**

Release	Modification
Cisco IOS XE Everest 16.5.1a	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 terminology are listed in the following table.

**Table 4: IPX Filtering Criteria**

IPX Encapsulation Type		Filter Criterion
Cisco IOS Name	Novell 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 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(config-ext-macl)# permit any host 00c0.00a0.03fa netbios
```

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

```
Device(config-ext-macl)# no permit any 00c0.00a0.03fa 0000.0000.0000 netbios
```

This example permits all packets with EtherType 0x4321:

```
Device(config-ext-macl)# permit any any 0x4321 0
```

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

#### Related Commands

Command	Description
<b>deny</b>	Denies from the MAC access-list configuration. Denies non-IP traffic to be forwarded if conditions are matched.
<b>mac access-list extended</b>	Creates an access list based on MAC addresses for non-IP traffic.

Command	Description
show access-lists	Displays access control lists configured on a switch.

## propagate sgt (cts manual)

To enable Security Group Tag (SGT) propagation at Layer 2 on Cisco TrustSec Security (CTS) interfaces, use the **propagate sgt** command in interface configuration mode. To disable SGT propagation, use the **no** form of this command.

### propagate sgt

#### Syntax Description

This command has no arguments or keywords.

#### Command Default

SGT processing propagation is enabled.

#### Command Modes

CTS manual interface configuration mode (config-if-cts-manual)

#### Command History

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

#### Usage Guidelines

SGT processing propagation allows a CTS-capable interface to accept and transmit a CTS Meta Data (CMD) based L2 SGT tag. The **no propagate sgt** command can be used to disable SGT propagation on an interface in situations where a peer device is not capable of receiving an SGT, and as a result, the SGT tag cannot be put in the L2 header.

#### Examples

The following example shows how to disable SGT propagation on a manually-configured TrustSec-capable interface:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet 0
Switch(config-if)# cts manual
Switch(config-if-cts-manual)# no propagate sgt
```

The following example shows that SGT propagation is disabled on Gigabit Ethernet interface 0:

```
Switch#show cts interface brief
Global Dot1x feature is Disabled
Interface GigabitEthernet0:
  CTS is enabled, mode:      MANUAL
  IFC state:                 OPEN
  Authentication Status:    NOT APPLICABLE
  Peer identity:             "unknown"
  Peer's advertised capabilities: ""
  Authorization Status:     NOT APPLICABLE
  SAP Status:                NOT APPLICABLE
  Propagate SGT:            Disabled
  Cache Info:
    Cache applied to link : NONE
```

#### Related Commands

Command	Description
<b>cts manual</b>	Enables an interface for CTS.

Command	Description
show cts interface	Displays Cisco TrustSec states and statistics per interface.

## protocol (IPv6 snooping)

To specify that addresses should be gleaned with Dynamic Host Configuration Protocol (DHCP) or Neighbor Discovery Protocol (NDP), or to associate the protocol with an IPv6 prefix list, use the **protocol** command. To disable address gleaning with DHCP or NDP, use the **no** form of the command.

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

<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				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.5.1a</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.5.1a	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.5.1a	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, place the switch in IPv6 snooping policy configuration mode, and configure the port to use DHCP to glean addresses:

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# protocol dhcp
```

# radius server



**Note** Starting from Cisco IOS 15.2(5)E release, the **radius server** command replaces the **radius-server host** command, being used in releases prior to Cisco IOS Release 15.2(5)E. The old command has been deprecated.

Use the **radius server** configuration sub-mode command on the switch stack or on a standalone switch to configure the RADIUS server parameters, including the RADIUS accounting and authentication. 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> } <i>ip{address   hostname}</i>	Specify the IP address of the RADIUS server.
<b>auth-port</b> <i>udp-port</i>	(Optional) Specify the UDP port for the RADIUS authentication server. The range is from 0 to 65536.
<b>acct-port</b> <i>udp-port</i>	(Optional) Specify the UDP port for the RADIUS accounting server. The range is from 0 to 65536.
<b>key</b> <i>string</i>	(Optional) Specify the authentication and encryption key for all RADIUS communication between the switch and the RADIUS daemon.  <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) Enable 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 Switch waits for the RADIUS server to reply before sending a request again. The range is 1 to 1000. This setting overrides the radius-server timeout global configuration command setting.
<b>no radius server</b> <i>name</i>	Returns to the default settings



**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**

Radius server sub-mode configuration

**Command History**

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced to replace the <b>radius-server host</b> command.

**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** sub-mode configuration command. 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(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
```

## sap mode-list (cts manual)

To select the Security Association Protocol (SAP) authentication and encryption modes (prioritized from highest to lowest) used to negotiate link encryption between two interfaces, use the **sap mode-list** command in CTS dot1x interface configuration mode. To remove a mode-list and revert to the default, use the **no** form of this command.

Use the **sap mode-list** command to manually specify the Pairwise Master Key (PMK) and the Security Association Protocol (SAP) authentication and encryption modes to negotiate MACsec link encryption between two interfaces. Use the **no** form of the command to disable the configuration.

**sap pmk mode-list** {gcm-encrypt | gmac | no-encap | null} [gcm-encrypt | gmac | no-encap | null]

**no sap pmk mode-list** {gcm-encrypt | gmac | no-encap | null} [gcm-encrypt | gmac | no-encap | null]

### Syntax Description

<b>pmk</b> <i>hex_value</i>	Specifies the Hex-data PMK (without leading 0x; enter even number of hex characters, or else the last character is prefixed with 0.).
<b>mode-list</b>	Specifies the list of advertised modes (prioritized from highest to lowest).
<b>gcm-encrypt</b>	Specifies GMAC authentication, GCM encryption.
<b>gmac</b>	Specifies GMAC authentication only, no encryption.
<b>no-encap</b>	Specifies no encapsulation.
<b>null</b>	Specifies encapsulation present, no authentication, no encryption.

### Command Default

The default encryption is **sap pmk mode-list gcm-encrypt null**. When the peer interface does not support 802.1AE MACsec or 802.REV layer-2 link encryption, the default encryption is **null**.

### Command Modes

CTS manual interface configuration (config-if-cts-manual)

### Command History

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

### Usage Guidelines

Use the **sap pmk mode-list** command to specify the authentication and encryption method.

The Security Association Protocol (SAP) is an encryption key derivation and exchange protocol based on a draft version of the 802.11i IEEE protocol. SAP is used to establish and maintain the 802.1AE link-to-link encryption (MACsec) between interfaces that support MACsec.

SAP and the Pairwise Master Key (PMK) can be manually configured between two interfaces with the **sap pmk mode-list** command. When using 802.1X authentication, both sides (supplicant and authenticator) receive the PMK and the MAC address of the peer's port from the Cisco Secure Access Control Server.

If a device is running CTS-aware software but the hardware is not CTS-capable, disallow encapsulation with the **sap mode-list no-encap** command.

### Examples

The following example shows how to configure SAP on a Gigabit Ethernet interface:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet 2/1
Switch(config-if)# cts manual
Switch(config-if-cts-manual)# sap pmk FFE0 mode-list gcm-encrypt
```

### Related Commands

Command	Description
<b>cts manual</b>	Enables an interface for CTS.
<b>propagate sgt (cts manual)</b>	Enables Security Group Tag (SGT) propagation at Layer 2 on Cisco TrustSec Security (CTS) interfaces.
<b>show cts interface</b>	Displays Cisco TrustSec interface configuration statistics.

## security level (IPv6 snooping)

To specify the level of security enforced, use the **security-level** command in IPv6 snooping policy configuration mode.

**security level** {**glean** | **guard** | **inspect**}

Syntax Description	<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.
Command Default	The default security level is guard.	
Command Modes	IPv6 snooping configuration	
Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

This example shows how to define an IPv6 snooping policy name as policy1, place the device in IPv6 snooping configuration mode, and configure the security level as inspect:

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# security-level inspect
```

# security passthru

To modify the IPsec pass-through, use the **security passthru** command. To disable, use the no form of the command.

```
security passthru ip-address
no security passthru
```

<b>Syntax Description</b>	<i>ip-address</i> IP address of the IPsec gateway (router) that is terminating the VPN tunnel.				
<b>Command Default</b>	None.				
<b>Command Modes</b>	wlan				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.5.1a</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.5.1a	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.5.1a	This command was introduced.				
<b>Usage Guidelines</b>	None.				

This example shows how to modify IPsec pass-through.

```
Device#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)#security passthrough 10.1.1.1
```

## 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 router 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 router 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.  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 16.5.1a	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
```

**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.

# show aaa clients

To show 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	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

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

```
Device# show aaa clients
Dropped request packets: 0
```



# show aaa command handler

To show AAA command handler statistics, use the **show aaa command handler** command.

## show aaa command handler

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

**Command Modes** User EXEC

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	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-logoff: 0
  account-query: 0, pod: 0
  service-logon: 0, service-logoff: 0
  user-profile-push: 0, session-state-log: 0
  reauthenticate: 0, bounce-host-port: 0
  disable-host-port: 0, update-rbacl: 0
  update-sgt: 0, update-cts-policies: 0
  invalid commands: 0
  async message not sent: 0
```

# show aaa local

To show 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

## Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	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
    Fail:                              0
```

## show aaa servers

To shows all AAA servers as seen by the AAA server MIB, use the **show aaa servers** command.

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

Syntax Description		
	<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.
Command Modes	User EXEC	
Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

This is an example of 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 show AAA sessions as seen by the AAA Session MIB, use the **show aaa sessions** command.

## show aaa sessions

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

**Command Modes** User EXEC

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

This is an example of 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}]
```

Syntax Description		
	<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.

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

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	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 5: 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 history

To display the authenticated sessions alive on the device, use the **show authentication history** command.

**show authentication history** [**min-uptime** *seconds*]

## Syntax Description

**min-uptime** *seconds* (Optional) Displays sessions within the minimum uptime. The range is from 1 through 4294967295 seconds.

## Command Modes

User EXEC

## Command History

### Release

Cisco IOS XE Everest 16.5.1a

### Modification

This command was introduced.

## Usage Guidelines

Use the **show authentication history** command to display the authenticated sessions alive on the device.

This is an example of output from the **show authentication history** command:

```
Device# show authentication history
Interface  MAC Address      Method  Domain  Status  Uptime
Gi3/0/2   0021.d864.07c0  dot1x   DATA   Auth    38s

Session count = 1
```



## 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

### Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	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 6: 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 7: 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 switch:

```
Device# show authentication sessions
Interface  MAC Address  Method  Domain  Status  Session ID
Gi1/0/48   0015.63b0.f676  dot1x   DATA   Authz Success  0A3462B1000000102983C05C
Gi1/0/5    000f.23c4.a401  mab     DATA   Authz Success  0A3462B10000000D24F80B58
Gi1/0/5    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: 0A3462C8000000000002763C
      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
      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 cts interface

To display Cisco TrustSec (CTS) configuration statistics for an interface, use the **show cts interface** command in EXEC or privileged EXEC mode.

**show cts interface** [{*type slot/port* | **brief** | **summary**}]

## Syntax Description

<b>type</b> <i>slot/port</i>	(Optional) Specifies an interface type and slot or port number. A verbose output for this interface is returned.
<b>brief</b>	(Optional) Displays abbreviated status for all CTS interfaces.
<b>summary</b>	(Optional) Displays a tabular summary of all CTS interfaces with 4 or 5 key status fields for each interface.

## Command Default

None

## Command Modes

EXEC (>)  
Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was modified with additional options.
Cisco IOS XE Denali 16.2.1	This command was introduced.

## Usage Guidelines

Use the **show cts interface** command without keywords to display verbose status for all CTS interfaces.

## Examples

The following example displays output without using a keyword (verbose status for all CTS interfaces):

```
Switch# show cts interface

Global Dot1x feature is Disabled
Interface GigabitEthernet0/1/0:
  CTS is enabled, mode:    MANUAL
  IFC state:              OPEN
  Interface Active for 00:00:18.232
  Authentication Status:  NOT APPLICABLE
  Peer identity:         "unknown"
  Peer's advertised capabilities: ""
  Authorization Status:   NOT APPLICABLE
  SAP Status:            NOT APPLICABLE
  Configured pairwise ciphers:
    gcm-encrypt
    null

  Replay protection:      enabled
  Replay protection mode: STRICT

  Selected cipher:
```

```

Propagate SGT:          Enabled
Cache Info:
  Cache applied to link : NONE

Statistics:
  authc success:        0
  authc reject:         0
  authc failure:        0
  authc no response:    0
  authc logoff:         0
  sap success:          0
  sap fail:             0
  authz success:        0
  authz fail:           0
  port auth fail:      0
Ingress:
  control frame bypassed: 0
  sap frame bypassed:    0
  esp packets:           0
  unknown sa:            0
  invalid sa:            0
  inverse binding failed: 0
  auth failed:           0
  replay error:         0
Egress:
  control frame bypassed: 0
  esp packets:           0
  sgt filtered:          0
  sap frame bypassed:    0
  unknown sa dropped:    0
  unknown sa bypassed:   0

```

The following example displays output using the **brief** keyword:

```

Device# show cts interface brief

Global Dot1x feature is Disabled
Interface GigabitEthernet0/1/0:
  CTS is enabled, mode:    MANUAL
  IFC state:              OPEN
  Interface Active for 00:00:40.386
  Authentication Status:  NOT APPLICABLE
  Peer identity:          "unknown"
  Peer's advertised capabilities: ""
  Authorization Status:   NOT APPLICABLE
  SAP Status:             NOT APPLICABLE
  Propagate SGT:         Enabled
  Cache Info:
    Cache applied to link : NONE

```

Related Commands	Command	Description
	<b>cts manual</b>	Enables an interface for CTS.
	<b>propagate sgt (cts manual)</b>	Enables Security Group Tag (SGT) propagation at Layer 2 on Cisco TrustSec Security (CTS) interfaces.
	<b>sap mode-list (cts manual)</b>	Manually specifies the PMK and the SAP authentication and encryption modes to negotiate MACsec link encryption between two interfaces.

# show cts role-based permissions

To display the role-based (security group) access control permission list, use the **show cts role-based permissions** command in privileged EXEC mode.

```
show cts role-based permissions [{default [{details | ipv4 [{details}]}] | from [{sgt [{ipv4 | to [{sgt | unknown}] [{details | ipv4 [{details}]}]}] | unknown}] | ipv4 | to [{sgt | unknown}] [{ipv4}]}
```

Syntax Description	
<b>default</b>	(Optional) Displays information about the default permission list.
<b>details</b>	(Optional) Displays attached access control list (ACL) details.
<b>ipv4</b>	(Optional) Displays information about the IPv4 protocol.
<b>from</b>	(Optional) Displays information about the source group.
<i>sgt</i>	(Optional) Security Group Tag. Valid values are from 2 to 65519.
<b>to</b>	(Optional) Displays information about the destination group.
<b>unknown</b>	(Optional) Displays information about unknown source and destination groups.

**Command Modes** Privileged EXE (#)

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

**Usage Guidelines** This command displays the content of the SGACL permission matrix. You can specify the source security group tag (SGT) by using the **from** keyword and the destination SGT by using the **to** keyword. When both these keywords are specified RBACLs of a single cell are displayed. An entire column is displayed when only the **to** keyword is used. An entire row is displayed when the **from** keyword is used. The entire permission matrix is displayed when both the **from** and **to** keywords are omitted.

The command output is sorted by destination SGT as a primary key and the source SGT as a secondary key. SGACLs for each cell is displayed in the same order they are defined in the configuration or acquired from Cisco Identity Services Engine (ISE).

The **details** keyword is provided when a single cell is selected by specifying both **from** and **to** keywords. When the **details** keyword is specified the access control entries of SGACLs of a single cell are displayed.

The following is sample output from the **show role-based permissions** command:

```
Switch# show cts role-based permissions

IPv4 Role-based permissions default (monitored):
default_sgacl-02
Permit IP-00
IPv4 Role-based permissions from group 305:sgt to group 306:dgt (monitored):
test_reg_tcp_permit-02
RBACL Monitor All for Dynamic Policies : TRUE
RBACL Monitor All for Configured Policies : FALSE
```

```
IPv4 Role-based permissions from group 6:SGT_6 to group 6:SGT_6 (configured):  
  mon_1  
IPv4 Role-based permissions from group 10 to group 11 (configured):  
  mon_2  
RBACL Monitor All for Dynamic Policies : FALSE  
RBACL Monitor All for Configured Policies : FALSE
```

**Related Commands**

Command	Description
<b>cts role-based permissions</b>	Enables permissions from a source group to a destination group.
<b>cts role-based monitor</b>	Enables role-based access list monitoring.

# show cisp

To display 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. Valid interfaces include physical ports and port channels.
<b>registrations</b>		Displays CISP registrations.
<b>summary</b>		(Optional) Displays CISP summary.
<b>Command Modes</b>	Privileged EXEC	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Everest 16.5.1a	This command was introduced.
		This command was reintroduced. This command was not supported in and

This example shows output from the **show cisp interface** command:

```
Device# show cisp interface fast 0
CISP not enabled on specified interface
```

This example shows 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**

<b>Command</b>	<b>Description</b>
<b>cisp enable</b>	Enable Client Information Signalling Protocol (CISP)
<b>dot1x credentials <i>profile</i></b>	Configure a profile on a supplicant switch

# show dot1x

To display IEEE 802.1x statistics, administrative status, and operational status for the switch or for the specified port, use the **show dot1x** command in user 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 type number</b>	(Optional) Displays the IEEE 802.1x status for the specified port.	

**Command Modes** User EXEC

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

This is an example of output from the **show dot1x all** command:

```
Device# show dot1x all
Sysauthcontrol           Enabled
Dot1x Protocol Version   3
```

This is an example of 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
```

This is an example of 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 16.5.1a	This command was introduced.

This is an example of output from the **show eap pac peers** privileged EXEC command:

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

### Related Commands

Command	Description
<b>clear eap sessions</b>	Clears EAP session information for the switch or for the specified port.

# 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 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				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.5.1a</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Everest 16.5.1a	This command was introduced.
Release	Modification				
Cisco IOS XE Everest 16.5.1a	This command was introduced.				
<b>Usage Guidelines</b>	In a switch stack, all statistics are generated on the stack master. If a new active switch is elected, the statistics counters reset.				

This is an example of 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
```

This is an example of 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**

<b>DHCP Snooping Statistic</b>	<b>Description</b>
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 switch 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.

<b>DHCP Snooping Statistic</b>	<b>Description</b>
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.

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

## Syntax Description

<i>name</i>	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.

## Command Modes

User EXEC  
Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

## Usage Guidelines

Use the **show radius server-group** command to display the server groups that you defined by using the **aaa group server radius** command.

This is an example of output from the **show radius server-group all** 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.
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".



Field	Description
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 storm-control

To display broadcast, multicast, or unicast storm control settings on the switch or on the specified interface or to display storm-control history, use the **show storm-control** command in user EXEC mode.

**show storm-control** [*interface-id*] [**broadcast** | **multicast** | **unicast**]

Syntax Description	
<i>interface-id</i>	(Optional) Interface ID for the physical port (including type, stack member for stacking-capable switches, module, and port number).
<b>broadcast</b>	(Optional) Displays broadcast storm threshold setting.
<b>multicast</b>	(Optional) Displays multicast storm threshold setting.
<b>unicast</b>	(Optional) Displays unicast storm threshold setting.

**Command Modes** User EXEC

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

**Usage Guidelines**

When you enter an interface ID, the storm control thresholds appear for the specified interface.

If you do not enter an interface ID, settings appear for one traffic type for all ports on the switch.

If you do not enter a traffic type, settings appear for broadcast storm control.

This is an example of a partial output from the **show storm-control** command when no keywords are entered. Because no traffic-type keyword was entered, the broadcast storm control settings appear.

```
Device> show storm-control
Interface Filter State Upper Lower Current
-----
Gi1/0/1 Forwarding 20 pps 10 pps 5 pps
Gi1/0/2 Forwarding 50.00% 40.00% 0.00%
<output truncated>
```

This is an example of output from the **show storm-control** command for a specified interface. Because no traffic-type keyword was entered, the broadcast storm control settings appear.

```
Device> show storm-control gigabitethernet 1/0/1
Interface Filter State Upper Lower Current
-----
Gi1/0/1 Forwarding 20 pps 10 pps 5 pps
```

The following table describes the fields in the show storm-control display:

**Table 10: show storm-control Field Descriptions**

Field	Description
Interface	Displays the ID of the interface.

Field	Description
Filter State	Displays the status of the filter: <ul style="list-style-type: none"><li>• Blocking—Storm control is enabled, and a storm has occurred.</li><li>• Forwarding—Storm control is enabled, and no storms have occurred.</li><li>• Inactive—Storm control is disabled.</li></ul>
Upper	Displays the rising suppression level as a percentage of total available bandwidth in packets per second or in bits per second.
Lower	Displays the falling suppression level as a percentage of total available bandwidth in packets per second or in bits per second.
Current	Displays the bandwidth usage of broadcast traffic or the specified traffic type (broadcast, multicast, or unicast) as a percentage of total available bandwidth. This field is only valid when storm control is enabled.

## 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 Default</b>	None	
<b>Command Modes</b>	Privileged EXEC	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

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

```
Device# show vlan access-map
Vlan access-map "vmap4" 10
  Match clauses:
    ip address: a12
  Action:
    forward
Vlan access-map "vmap4" 20
  Match clauses:
    ip address: a12
  Action:
    forward
```

# show vlan filter

To display information about all VLAN filters or about a particular VLAN or VLAN access map, use the **show vlan filter** command in privileged EXEC mode.

```
show vlan filter {access-map name | vlan vlan-id}
```

<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 Default</b>	None	
<b>Command Modes</b>	Privileged EXEC	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

This is an example of output from the **show vlan filter** command:

```
Device# show vlan filter
VLAN Map map_1 is filtering VLANs:
 20-22
```

# show vlan group

To display the VLANs that are mapped to VLAN groups, use the **show vlan group** command in privileged EXEC mode.

```
show vlan group [{group-name vlan-group-name [user_count]]
```

## Syntax Description

**group-name** *vlan-group-name* (Optional) Displays the VLANs mapped to the specified VLAN group.

**user\_count** (Optional) Displays the number of users in each VLAN mapped to a specified VLAN group.

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

### Release

Cisco IOS XE Everest 16.5.1a

### Modification

This command was introduced.

## Usage Guidelines

The **show vlan group** command displays the existing VLAN groups and lists the VLANs and VLAN ranges that are members of each VLAN group. If you enter the **group-name** keyword, only the members of the specified VLAN group are displayed.

This example shows how to display the members of a specified VLAN group:

## storm-control

To enable broadcast, multicast, or unicast storm control and to set threshold levels on an interface, use the **storm-control** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

```
storm-control {action {shutdown | trap} | {broadcast | multicast | unicast} level {level [level-low] |
bps bps [bps-low] | pps pps [pps-low]}}
no storm-control {action {shutdown | trap} | {broadcast | multicast | unicast} level}
```

### Syntax Description

<b>action</b>	Specifies the action taken when a storm occurs on a port. The default action is to filter traffic and to not send an Simple Network Management Protocol (SNMP) trap.
<b>shutdown</b>	Disables the port during a storm.
<b>trap</b>	Sends an SNMP trap when a storm occurs.
<b>broadcast</b>	Enables broadcast storm control on the interface.
<b>multicast</b>	Enables multicast storm control on the interface.
<b>unicast</b>	Enables unicast storm control on the interface.
<b>level</b>	Specifies the rising and falling suppression levels as a percentage of total bandwidth of the port.
<i>level</i>	Rising suppression level, up to two decimal places. The range is 0.00 to 100.00. Block the flooding of storm packets when the value specified for level is reached.
<i>level-low</i>	(Optional) Falling suppression level, up to two decimal places. The range is 0.00 to 100.00. This value must be less than or equal to the rising suppression value. If you do not configure a falling suppression level, it is set to the rising suppression level.
<b>level bps</b>	Specifies the rising and falling suppression levels as a rate in bits per second at which traffic is received on the port.
<i>bps</i>	Rising suppression level, up to 1 decimal place. The range is 0.0 to 10000000000.0. Block the flooding of storm packets when the value specified for bps is reached. You can use metric suffixes such as k, m, and g for large number thresholds.
<i>bps-low</i>	(Optional) Falling suppression level, up to 1 decimal place. The range is 0.0 to 10000000000.0. This value must be equal to or less than the rising suppression value. You can use metric suffixes such as k, m, and g for large number thresholds.
<b>level pps</b>	Specifies the rising and falling suppression levels as a rate in packets per second at which traffic is received on the port.
<i>pps</i>	Rising suppression level, up to 1 decimal place. The range is 0.0 to 10000000000.0. Block the flooding of storm packets when the value specified for pps is reached. You can use metric suffixes such as k, m, and g for large number thresholds.

*pps-low* (Optional) Falling suppression level, up to 1 decimal place. The range is 0.0 to 10000000000.0. This value must be equal to or less than the rising suppression value.

You can use metric suffixes such as k, m, and g for large number thresholds.

#### Command Default

Broadcast, multicast, and unicast storm control are disabled.

The default action is to filter traffic and to not send an SNMP trap.

#### Command Modes

Interface configuration

#### Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

#### Usage Guidelines

The storm-control suppression level can be entered as a percentage of total bandwidth of the port, as a rate in packets per second at which traffic is received, or as a rate in bits per second at which traffic is received.

When specified as a percentage of total bandwidth, a suppression value of 100 percent means that no limit is placed on the specified traffic type. A value of **level 0 0** means that all broadcast, multicast, or unicast traffic on that port is blocked. Storm control is enabled only when the rising suppression level is less than 100 percent. If no other storm-control configuration is specified, the default action is to filter the traffic causing the storm and to send no SNMP traps.



#### Note

When the storm control threshold for multicast traffic is reached, all multicast traffic except control traffic, such as bridge protocol data unit (BPDU) and Cisco Discovery Protocol (CDP) frames, are blocked. However, the switch does not differentiate between routing updates, such as Open Shortest Path First (OSPF) and regular multicast data traffic, so both types of traffic are blocked.

The **trap** and **shutdown** options are independent of each other.

If you configure the action to be taken as shutdown (the port is error-disabled during a storm) when a packet storm is detected, you must use the **no shutdown** interface configuration command to bring the interface out of this state. If you do not specify the **shutdown** action, specify the action as **trap** (the switch generates a trap when a storm is detected).

When a storm occurs and the action is to filter traffic, if the falling suppression level is not specified, the switch blocks all traffic until the traffic rate drops below the rising suppression level. If the falling suppression level is specified, the switch blocks traffic until the traffic rate drops below this level.



#### Note

Storm control is supported on physical interfaces. You can also configure storm control on an EtherChannel. When storm control is configured on an EtherChannel, the storm control settings propagate to the EtherChannel physical interfaces.

When a broadcast storm occurs and the action is to filter traffic, the switch blocks only broadcast traffic.

For more information, see the software configuration guide for this release.



This example shows how to enable broadcast storm control with a 75.5-percent rising suppression level:

```
Device(config-if)# storm-control broadcast level 75.5
```

This example shows how to enable unicast storm control on a port with a 87-percent rising suppression level and a 65-percent falling suppression level:

```
Device(config-if)# storm-control unicast level 87 65
```

This example shows how to enable multicast storm control on a port with a 2000-packets-per-second rising suppression level and a 1000-packets-per-second falling suppression level:

```
Device(config-if)# storm-control multicast level pps 2k 1k
```

This example shows how to enable the **shutdown** action on a port:

```
Device(config-if)# storm-control action shutdown
```

You can verify your settings by entering the **show storm-control** privileged EXEC command.

## 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> <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

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	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(config)# interface gigabitethernet1/0/1
Device(config-if)# switchport port-security aging time 120
```

This example sets the aging time as 2 minutes for inactivity aging type with aging enabled for configured secure addresses on the port:

```
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
```

This example shows how to disable aging for configured secure addresses:

```
Device(config)# interface gigabitethernet1/0/2  
Device(config-if)# no switchport port-security aging static
```

## 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

**mac-address** 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.

**vlan vlan-id** (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.

**vlan access** (Optional) On an access port only, specifies the VLAN as an access VLAN.

**vlan voice** (Optional) On an access port only, specifies the VLAN as a voice VLAN.

**Note** The **voice** keyword is available only if voice VLAN is configured on a port and if that port is not the access VLAN.

**sticky** 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.

**mac-address** (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

### Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	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 switch 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** privileged EXEC command.

This example shows how to configure a secure MAC address and a VLAN ID on a port:

```
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
```

This example shows how to enable sticky learning and to enter two sticky secure MAC addresses on a port:

```
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
```

# 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

**value** Sets the maximum number of secure MAC addresses for the interface.  
The default setting is 1.

**vlan** (Optional) For trunk ports, sets the maximum number of secure MAC addresses on a VLAN or range of VLANs. If the **vlan** keyword is not entered, the default value is used.

**vlan-list** (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.

**access** (Optional) On an access port only, specifies the VLAN as an access VLAN.

**voice** (Optional) On an access port only, specifies the VLAN as a voice VLAN.

**Note** The **voice** 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

## Command History

### Release

### Modification

Cisco IOS XE Everest 16.5.1a

This command was introduced.

## Usage Guidelines

The maximum number of secure MAC addresses that you can configure on a switch or switch stack 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** privileged EXEC 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(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
```

## 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}
```

Syntax Description		
	<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.

**Command Default** The default violation mode is **shutdown**.

**Command Modes** Interface configuration

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

**Usage Guidelines** 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 show how to configure a port to shut down only the VLAN if a MAC security violation occurs:

```
Device(config)# interface gigabitethernet2/0/2  
Device(config)# switchport port-security violation shutdown vlan
```

## 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**

<b>Syntax Description</b>	<b>name</b> Name of the private TACACS+ server host.
---------------------------	--

**Command Default** No TACACS+ server is configured.

**Command Modes** Global configuration (config)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Everest 16.5.1a	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(config)# tacacs server server1
Device(config-server-tacacs)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<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	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Everest 16.5.1a	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, place the switch in IPv6 snooping policy configuration mode, and configure an entry to stay in the binding table for an infinite length of time on a trusted port:

```
Device(config)# ipv6 snooping policy policy1  
Device(config-ipv6-snooping)# tracking disable stale-lifetime infinite
```

## trusted-port

To configure a port to become a trusted port, use the **trusted-port** command in IPv6 snooping policy mode or ND inspection policy configuration mode. To disable this function, use the **no** form of this command.

**trusted-port**  
**no trusted-port**

---

### Syntax Description

This command has no arguments or keywords.

---

### Command Default

No ports are trusted.

---

### Command Modes

ND inspection policy configuration  
 IPv6 snooping configuration

---

### Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

---

### Usage Guidelines

When the **trusted-port** command is enabled, limited or no verification is performed when messages are received on ports that have this policy. However, to protect against address spoofing, messages are analyzed so that the binding information that they carry can be used to maintain the binding table. Bindings discovered from these ports will be considered more trustworthy than bindings received from ports that are not configured to be trusted.

This example shows how to define an NDP policy name as policy1, place the switch in NDP inspection policy configuration mode, and configure the port to be trusted:

```
Device(config)# ipv6 nd inspection policy1
Device(config-nd-inspection)# trusted-port
```

This example shows how to define an IPv6 snooping policy name as policy1, place the switch in IPv6 snooping policy configuration mode, and configure the port to be trusted:

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# trusted-port
```

# vlan access-map

To create or modify a VLAN map entry for VLAN packet filtering, and change the mode to the VLAN access-map configuration, use the **vlan access-map** command in global configuration mode on the switch stack or on a standalone switch. To delete a VLAN map entry, use the **no** form of this command.

```
vlan access-map name [number]
no vlan access-map name [number]
```



## Note

This command is not supported on switches running the LAN Base feature set.

## Syntax Description

<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.

## Command Default

There are no VLAN map entries and no VLAN maps applied to a VLAN.

## Command Modes

Global configuration

## Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

## Usage Guidelines

In global configuration mode, use this command to create or modify a VLAN map. This entry changes the mode to VLAN access-map configuration, where you can use the **match** access-map configuration command to specify the access lists for IP or non-IP traffic to match and use the **action** command to set whether a match causes the packet to be forwarded or dropped.

In VLAN access-map configuration mode, these commands are available:

- **action**—Sets the action to be taken (forward or drop).
- **default**—Sets a command to its defaults.
- **exit**—Exits from VLAN access-map configuration mode.
- **match**—Sets the values to match (IP address or MAC address).
- **no**—Negates a command or set its defaults.

When you do not specify an entry number (sequence number), it is added to the end of the map.

There can be only one VLAN map per VLAN and it is applied as packets are received by a VLAN.

You can use the **no vlan access-map name [number]** command with a sequence number to delete a single entry.

Use the **vlan filter** interface configuration command to apply a VLAN map to one or more VLANs. For more information about VLAN map entries, see the software configuration guide for this release.

This example shows how to create a VLAN map named vac1 and apply matching conditions and actions to it. If no other entries already exist in the map, this will be entry 10.

```
Device(config)# vlan access-map vac1  
Device(config-access-map)# match ip address acl1  
Device(config-access-map)# action forward
```

This example shows how to delete VLAN map vac1:

```
Device(config)# no vlan access-map vac1
```

# vlan 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 on the switch stack or on a standalone switch. To remove the map, use the **no** form of this command.

```
vlan filter mapname vlan-list {list | all}
no vlan filter mapname vlan-list {list | all}
```



**Note** This command is not supported on switches running the LAN Base feature set.

## Syntax Description

<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.

## Command Default

There are no VLAN filters.

## Command Modes

Global configuration

## Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

## Usage Guidelines

To avoid accidentally dropping too many packets and disabling connectivity in the middle of the configuration process, we recommend that you completely define the VLAN access map before applying it to a VLAN.

For more information about VLAN map entries, see the software configuration guide for this release.

This example applies VLAN map entry map1 to VLANs 20 and 30:

```
Device(config)# vlan filter map1 vlan-list 20, 30
```

This example shows how to delete VLAN map entry mac1 from VLAN 20:

```
Device(config)# no vlan filter map1 vlan-list 20
```

You can verify your settings by entering the **show vlan filter** privileged EXEC command.

# vlan group

To create or modify a VLAN group, use the **vlan group** command in global configuration mode. To remove a VLAN list from the VLAN group, use the **no** form of this command.

```
vlan group group-name vlan-list vlan-list
no vlan group group-name vlan-list vlan-list
```

## Syntax Description

<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 Default

None

## Command Modes

Global configuration

## Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

## Usage Guidelines

If the named VLAN group does not exist, the **vlan group** command creates the group and maps the specified VLAN list to the group. If the named VLAN group exists, the specified VLAN list is mapped to the group.

The **no** form of the **vlan group** command removes the specified VLAN list from the VLAN group. When you remove the last VLAN from the VLAN group, the VLAN group is deleted.

A maximum of 100 VLAN groups can be configured, and a maximum of 4094 VLANs can be mapped to a VLAN group.

This example shows how to map VLANs 7 through 9 and 11 to a VLAN group:

```
Device(config)# vlan group group1 vlan-list 7-9,11
```

This example shows how to remove VLAN 7 from the VLAN group:

```
Device(config)# no vlan group group1 vlan-list 7
```