Security Commands

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

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

Command Default

AAA accounting is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	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.

Examples

This example shows how to configure IEEE 802.1x accounting:

```
Switch(config)# aaa new-model
Switch(config)# aaa accounting dot1x default start-stop group radius
```

aaa accounting identity

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

aaa accounting identity {*name* | **default** } **start-stop** {**broadcast group** {*name* | **radius** | **tacacs+**} [**group** {*name* | **radius** | **tacacs+**} ...] | **group** {*name* | **radius** | **tacacs+**} [**group** {*name* | **radius** | **tacacs+**}...]}

no aaa accounting identity {*name* | **default** }

Syntax Description

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

Command Default

AAA accounting is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	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.

Examples

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

```
Switch# 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.

Switch# configure terminal
Switch(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 the switch stack or on a standalone switch. To disable authentication, use the **no** form of this command.

aaa authentication dot1x {**default**} *method1*

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

Syntax Description

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

Command Default

No authentication is performed.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	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.

Examples

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.

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

aaa authorization network

To the 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

Syntax Description

default group radius	Use the list of all RADIUS hosts in the server group as the default authorization list.

Command Default

Authorization is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	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.

Examples

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

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

authentication host-mode

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

authentication host-mode {**multi-auth** | **multi-domain** | **multi-host** | **single-host**}

no authentication host-mode

Syntax Description

multi-auth	Enables multiple-authorization mode (multi-auth mode) on the port.
multi-domain	Enables multiple-domain mode on the port.
multi-host	Enables multiple-host mode on the port.
single-host	Enables single-host mode on the port.

Command Default

Single host mode is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	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.

Examples

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

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

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

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

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

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

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

```
Switch(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 switch, 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 enabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

The command enables authenticated hosts to move between ports on a switch. 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.

Examples

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

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

authentication priority

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

authentication priority [**dot1x** | **mab**] {**webauth**}

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

Syntax Description

dot1x	(Optional) Adds 802.1x to the order of authentication methods.
mab	(Optional) Adds MAC authentication bypass (MAB) to the order of authentication methods.
webauth	Adds web authentication to the order of authentication methods.

Command Default

The default priority is 802.1x authentication, followed by MAC authentication bypass and web authentication.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

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

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

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

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

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

Examples

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

```
Switch(config-if)# authentication priority dotx webauth
```

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

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

Related Commands

Command	Description
authentication control-direction	Configures the port mode as unidirectional or bidirectional.
authentication event fail	Specifies how the Auth Manager handles authentication failures as a result of unrecognized user credentials.
authentication event no-response action	Specifies how the Auth Manager handles authentication failures as a result of a nonresponsive host.
authentication event server alive action reinitialize	Reinitializes an authorized Auth Manager session when a previously unreachable authentication, authorization, and accounting server becomes available.
authentication event server dead action authorize	Authorizes Auth Manager sessions when the authentication, authorization, and accounting server becomes unreachable.
authentication fallback	Enables a web authentication fallback method.
authentication host-mode	Allows hosts to gain access to a controlled port.
authentication open	Enables open access on a port.
authentication order	Specifies the order in which the Auth Manager attempts to authenticate a client on a port.
authentication periodic	Enables automatic reauthentication on a port.
authentication port-control	Configures the authorization state of a controlled port.
authentication timer inactivity	Configures the time after which an inactive Auth Manager session is terminated.
authentication timer reauthenticate	Specifies the period of time between which the Auth Manager attempts to reauthenticate authorized ports.

Command	Description
authentication timer restart	Specifies the period of time after which the Auth Manager attempts to authenticate an unauthorized port.
authentication violation	Specifies the action to be taken when a security violation occurs on a port.
mab	Enables MAC authentication bypass on a port.
show authentication registrations	Displays information about the authentication methods that are registered with the Auth Manager.
show authentication sessions	Displays information about current Auth Manager sessions.
show authentication sessions interface	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

protect	Drops unexpected incoming MAC addresses. No syslog errors are generated.
replace	Removes the current session and initiates authentication with the new host.
restrict	Generates a syslog error when a violation error occurs.
shutdown	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 3.3SE	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.

Examples

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:

```
Switch(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:

```
Switch(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:

```
Switch(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:

```
Switch(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, 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 3.3SE	This command was introduced.

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.

Examples

This example shows how to enable CISP:

```
Switch(config)# cisp enable
```

Related Commands

Command	Description
dot1x credentials*profile*	Configures a profile on a supplicant switch.
dot1x supplicant force-multicast	Forces 802.1X supplicant to send multicast packets.
dot1x supplicant controlled transient	Configures controlled access by 802.1X supplicant.
show cisp	Displays CISP information for a specified interface.

clear errdisable interface vlan

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

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

Syntax Description

interface-id	Specifies an interface.
vlan list	(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 3.3SE	This command was introduced.

Usage Guidelines

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

Examples

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

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

Related Commands

Command	Description
errdisable detect cause	Enables error-disabled detection for a specific cause or all causes.
errdisable recovery	Configures the recovery mechanism variables.
show errdisable detect	Displays error-disabled detection status.
show errdisable recovery	Displays error-disabled recovery timer information.

Command	Description
show interfaces status err-disabled	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

dynamic	Deletes all dynamic MAC addresses.
address *mac-addr*	(Optional) Deletes the specified dynamic MAC address.
interface *interface-id*	(Optional) Deletes all dynamic MAC addresses on the specified physical port or port channel.
vlan *vlan-id*	(Optional) Deletes all dynamic MAC addresses for the specified VLAN. The range is 1 to 4094.
move update	Clears the MAC address table move-update counters.
notification	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 3.3SE	This command was introduced.

Usage Guidelines

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

Examples

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

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

Related Commands

Command	Description
mac address-table notification	Enables the MAC address notification feature.
mac address-table move update {**receive** | **transmit**}	Configures MAC address-table move update on the switch.
show mac address-table	Displays the MAC address table static and dynamic entries.
show mac address-table move update	Displays the MAC address-table move update information on the switch.
show mac address-table notification	Displays the MAC address notification settings for all interfaces or on the specified interface when the **interface** keyword is appended.
snmp trap mac-notification change	Enables the SNMP MAC address notification trap on a specific interface.

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** | **lavc-sca** | **lsap** *lsap mask* | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp**][**cos** *cos*]

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

Syntax Description

any	Denies any source or destination MAC address.
host *src-MAC-addr* | *src-MAC-addr mask*	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.
host *dst-MAC-addr* | *dst-MAC-addr mask*	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.
type mask	(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.
aarp	(Optional) Specifies EtherType AppleTalk Address Resolution Protocol that maps a data-link address to a network address.
amber	(Optional) Specifies EtherType DEC-Amber.
appletalk	(Optional) Specifies EtherType AppleTalk/EtherTalk.
dec-spanning	(Optional) Specifies EtherType Digital Equipment Corporation (DEC) spanning tree.
decnet-iv	(Optional) Specifies EtherType DECnet Phase IV protocol.
diagnostic	(Optional) Specifies EtherType DEC-Diagnostic.

dsm	(Optional) Specifies EtherType DEC-DSM.
etype-6000	(Optional) Specifies EtherType 0x6000.
etype-8042	(Optional) Specifies EtherType 0x8042.
lat	(Optional) Specifies EtherType DEC-LAT.
lavc-sca	(Optional) Specifies EtherType DEC-LAVC-SCA.
lsap *lsap-number mask*	(Optional) Specifies the LSAP number (0 to 65535) of a packet with 802.2 encapsulation to identify the protocol of the packet. *mask* is a mask of don't care bits applied to the LSAP number before testing for a match.
mop-console	(Optional) Specifies EtherType DEC-MOP Remote Console.
mop-dump	(Optional) Specifies EtherType DEC-MOP Dump.
msdos	(Optional) Specifies EtherType DEC-MSDOS.
mumps	(Optional) Specifies EtherType DEC-MUMPS.
netbios	(Optional) Specifies EtherType DEC- Network Basic Input/Output System (NetBIOS).
vines-echo	(Optional) Specifies EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems.
vines-ip	(Optional) Specifies EtherType VINES IP.
xns-idp	(Optional) Specifies EtherType Xerox Network Systems (XNS) protocol suite (0 to 65535), an arbitrary EtherType in decimal, hexadecimal, or octal.
cos *cos*	(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 **cos** 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 3.3SE	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 1: 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

Examples

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.

```
Switch(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:

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

This example denies all packets with EtherType 0x4321:

```
Switch(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
mac access-list extended	Creates an access list based on MAC addresses for non-IP traffic.
permit	Permits from the MAC access-list configuration. Permits non-IP traffic to be forwarded if conditions are matched.
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**}

Syntax Description

node	Sets the role of the attached device to node.
switch	Sets the role of the attached device to switch.

Command Default

The device role is node.

Command Modes

IPv6 snooping configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	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.

Examples

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:

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

device-role (IPv6 nd inspection)

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

device-role {**host** | **monitor** | **router** | **switch**}

Syntax Description

host	Sets the role of the attached device to host.
monitor	Sets the role of the attached device to monitor.
router	Sets the role of the attached device to router.
switch	Sets the role of the attached device to switch.

Command Default

The device role is host.

Command Modes

ND inspection policy configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	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. If the device role is enabled using the **router** keyword, all messages (router solicitation [RS], router advertisement [RA], or redirect) are allowed on this port.

When the **router** or **monitor** keyword is used, the multicast RS messages are bridged on the port, regardless of whether limited broadcast is enabled. However, the monitor keyword does not allow inbound RA or redirect messages. When the monitor keyword is used, devices that need these messages will receive them.

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

Examples

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:

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

dot1x critical (global configuration)

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

dot1x critical eapol

Syntax Description

eapol	Specifies that the switch send an EAPOL-Success message when the switch successfully authenticates the critical port.

Command Default

eapol is disabled

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Examples

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

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

dot1x pae

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

dot1x pae {**supplicant** | **authenticator**}

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

Syntax Description

supplicant	The interface acts only as a supplicant and will not respond to messages that are meant for an authenticator.
authenticator	The interface acts only as an authenticator and will not respond to any messages meant for a supplicant.

Command Default

PAE type is not set.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

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

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

Examples

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

```
Switch(config)# interface g1/0/3
Switch(config-if)# dot1x pae supplicant
```

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 3.3SE	This command was introduced.

Usage Guidelines

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

Examples

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

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

Related Commands

Command	Description
cisp enable	Enable Client Information Signalling Protocol (CISP) on a switch so that it acts as an authenticator to a supplicant switch.
dot1x credentials	Configure the 802.1x supplicant credentials on the port.
dot1x pae supplicant	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*]

Syntax Description

interface *interface-id*	(Optional) Port to be queried.

Command Default

There is no default setting.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.3SE	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.

Examples

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:

```
Switch# 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
```

Related Commands

Command	Description
dot1x test timeout *timeout*	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*

Syntax Description

timeout	Time in seconds to wait for an EAPOL response. The range is from 1 to 65535 seconds.

Command Default

The default setting is 10 seconds.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	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.

Examples

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

```
Switch# dot1x test timeout 27
```

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

Related Commands

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

auth-period *seconds*	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.
held-period *seconds*	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
quiet-period *seconds*	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
ratelimit-period *seconds*	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). • The authenticator ignores EAPOL-Start packets from clients that have successfully authenticated for the rate-limit period duration. • The range is from 1 to 65535. By default, rate limiting is disabled.
server-timeout *seconds*	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. If the server does not send a response to an 802.1X packet within the specified period, the packet is sent again.
start-period *seconds*	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.

supp-timeout *seconds*	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.
tx-period *seconds*	Configures the number of seconds between retransmission of EAP request ID packets (assuming that no response is received) to the client. • The range is from 1 to 65535. The default is 30. • 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.

Command Default

Periodic reauthentication and periodic rate-limiting are done.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	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.

Examples

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

```
Switch(config)# configure terminal
Switch(config)# interface g1/0/3
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x timeout auth-period 2000
Switch(config-if)# dot1x timeout held-period 2400
Switch(config-if)# dot1x timeout quiet-period 600
Switch(config-if)# dot1x timeout start-period 90
Switch(config-if)# dot1x timeout supp-timeout 300
Switch(config-if)# dot1x timeout tx-period 60
```

```
Switch(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 3.3SE	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.

Examples

This example shows how to configure an open directive.

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

Related Commands

Command	Description
show running-config	Displays the contents of the current running configuration file.

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 3.3SE	This command was introduced.

Usage Guidelines

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

Examples

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

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(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.

```
Switch# configure terminal
Switch(config)# fallback profile profile1
Switch(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

name	Name of network admission control rule.
consent	Associates an authentication proxy consent web page with the IP admission rule specified using the *admission-name* argument.
proxy http	Configures web authentication custom page.
absolute-timer *minutes*	(Optional) Elapsed time, in minutes, before the external server times out.
inactivity-time *minutes*	(Optional) Elapsed time, in minutes, before the external file server is deemed unreachable.
list	(Optional) Associates the named rule with an access control list (ACL).
acl	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.
acl-name	Applies a named access list to a named admission control rule.
service-policy type tag	(Optional) A control plane service policy is to be configured.
service-policy-name	Control plane tag service policy that is configured using the **policy-map type control tag***policyname* 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 3.3SE	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:

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

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

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

Related Commands

Command	Description
dot1x fallback	Configures a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
fallback profile	Creates a web authentication fallback profile.
ip admission	Enables web authentication on a port.
show authentication sessions interface *interface* **detail**	Displays information about the web authentication session status.

Command	Description
show ip admission	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

Syntax Description

number	Number of bindings created in the IP device tracking table for a port. The range is 0 (disabled) to 65535.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
Cisco IOS XE 3.3SE	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.

Examples

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

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

count *number*	Sets the number of times that the switch sends the ARP probe. The range is from 1 to 255.
delay *seconds*	Sets the number of seconds that the switch waits before sending the ARP probe. The range is from 1 to 120.
interval *seconds*	Sets the number of seconds that the switch waits for a response before resending the ARP probe. The range is from 30 to 1814400 seconds.
use-svi	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 3.3SE	This command was introduced.

Usage Guidelines

Use the **use-svi** 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:

```
Switch(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.

no ip dhcp snooping database [**timeout** | **write-delay**]

Syntax Description

flash:*url*	Specifies the database URL for storing entries using flash.
ftp:*url*	Specifies the database URL for storing entries using FTP.
http:*url*	Specifies the database URL for storing entries using HTTP.
https:*url*	Specifies the database URL for storing entries using secure HTTP (https).
rcp:*url*	Specifies the database URL for storing entries using remote copy (rcp).
scp:*url*	Specifies the database URL for storing entries using Secure Copy (SCP).
tftp:*url*	Specifies the database URL for storing entries using TFTP.
timeout *seconds*	Specifies the abort timeout interval; valid values are from 0 to 86400 seconds.
write-delay *seconds*	Specifies the amount of time before writing the DHCP-snooping entries to an external server after a change is seen in the local DHCP-snooping database; valid values are from 15 to 86400 seconds.

Command Default

The DHCP-snooping database is not configured.

Command Modes Global configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	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.

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

```
Switch(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:

```
Switch(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*}

Syntax Description

hostname	Specify the switch hostname as the remote ID.
string *string*	Specify a remote ID, using from 1 to 63 ASCII characters (no spaces).

Command Default

The switch MAC address is the remote ID.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

You must globally enable DHCP snooping by using the **ip dhcp snooping** global configuration command for any DHCP snooping configuration to take effect.

When the option-82 feature is enabled, the default remote-ID suboption is the 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.

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

Examples

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

```
Switch(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 3.3SE	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 reenable verification.

Examples

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

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

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*

Syntax Description

mac-address	Binding MAC address.
vlan *vlan-id*	Specifies the Layer 2 VLAN identification; valid values are from 1 to 4094.
ip-address	Binding IP address.
interface *interface-id*	ID of the physical interface.

Command Default

No IP source bindings are configured.

Command Modes

Global configuration.

Command History

Release	Modification
Cisco IOS XE 3.3SE	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.

Examples

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

```
Switch# configure terminal
Switchconfig) 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**]

no ip verify source

Syntax Description

mac-check	(Optional) Enables IP source guard with MAC address verification.

Command Default

IP source guard is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	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:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip verify source
```

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

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

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

ipv6 snooping policy

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

ipv6 snooping policy *snooping-policy*

no ipv6 snooping policy *snooping-policy*

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 3.3SE	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.

Examples

This example shows how to configure an IPv6 snooping policy:

```
Switch(config)# ipv6 snooping policy policy1
```

```
Switch(config-ipv6-snooping)#
```

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 3.3SE	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.

Examples

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:

```
Switch(config)# ipv6 nd inspection policy policy1
Switch(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:

```
Switch(config)# ipv6 snooping policy policy1
Switch(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 3.3SE	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.

Examples

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

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

Related Commands

Command	Description
authentication event	Sets the action for specific authentication events.
authentication fallback	Configures a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
authentication host-mode	Sets the authorization manager mode on a port.
authentication open	Enables or disables open access on a port.
authentication order	Sets the order of authentication methods used on a port.

Command	Description
authentication periodic	Enables or disables reauthentication on a port.
authentication port-control	Enables manual control of the port authorization state.
authentication priority	Adds an authentication method to the port-priority list.
authentication timer	Configures the timeout and reauthentication parameters for an 802.1x-enabled port.
authentication violation	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.
mab	Enables MAC-based authentication on a port.
mab eap	Configures a port to use the Extensible Authentication Protocol (EAP).
show authentication	Displays information about authentication manager events on the 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** {*name*| *number*} [*name*| *number*] [*name*| *number*]...| **mac address** {*name*} [*name*] [*name*]...}

no match {**ip address** {*name*| *number*} [*name*| *number*] [*name*| *number*]...| **mac address** {*name*} [*name*] [*name*]...}

Syntax Description

ip address	Sets the access map to match packets against an IP address access list.
mac address	Sets the access map to match packets against a MAC address access list.
name	Name of the access list to match packets against.
number	Number of the access list to match packets against. This option is not valid for MAC access lists.

Command Default

The default action is to have no match parameters applied to a VLAN map.

Command Modes

Access-map configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

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

You must enter one access list name or number; others are optional. You can match packets against one or more access lists. Matching any of the lists counts as a match of the entry.

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

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

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

Examples

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

```
Switch(config)# vlan access-map vmap4
Switch(config-access-map)# match ip address al2
Switch(config-access-map)# action drop
Switch(config-access-map)# exit
Switch(config)# vlan filter vmap4 vlan-list 5-6
```

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

no authentication logging verbose

To filter detailed information from authentication system messages, use the **no authentication logging verbose** command in global configuration mode on the switch stack or on a standalone switch.

no authentication logging verbose

Syntax Description

This command has no arguments or keywords.

Command Default

All details are displayed in the system messages.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

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

Examples

To filter verbose authentication system messages:

```
Switch(config)# no authentication logging verbose
```

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

Related Commands

Command	Description
no authentication logging verbose	Filters details from authentication system messages.
no dot1x logging verbose	Filters details from 802.1x system messages.
no mab logging verbose	Filters details from MAC authentication bypass (MAB) system messages.

no dot1x logging verbose

To filter detailed information from 802.1x system messages, use the **no dot1x logging verbose** command in global configuration mode on the switch stack or on a standalone switch.

no dot1x logging verbose

Syntax Description

This command has no arguments or keywords.

Command Default

All details are displayed in the system messages.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

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

Examples

To filter verbose 802.1x system messages:

```
Switch(config)# no dot1x logging verbose
```

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

Related Commands

Command	Description
no authentication logging verbose	Filters details from authentication system messages.
no dot1x logging verbose	Filters details from 802.1x system messages.
no mab logging verbose	Filters details from MAC authentication bypass (MAB) system messages.

no mab logging verbose

To filter detailed information from MAC authentication bypass (MAB) system messages, use the **no mab logging verbose** command in global configuration mode on the switch stack or on a standalone switch.

no mab logging verbose

Syntax Description

This command has no arguments or keywords.

Command Default

All details are displayed in the system messages.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	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.

Examples

To filter verbose MAB system messages:

```
Switch(config)# no mab logging verbose
```

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

Related Commands

Command	Description
no authentication logging verbose	Filters details from authentication system messages.
no dot1x logging verbose	Filters details from 802.1x system messages.
no mab logging verbose	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** | **host***src-MAC-addr* | *src-MAC-addr mask*} {**any** | **host***dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask* | **aarp** | **amber** | **appletalk** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **lsap***lsap mask* | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp**][**cos***cos*]

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** | **lavc-sca** | **lsap** *lsap mask* | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp**][**cos***cos*]

Syntax Description

any	Denies any source or destination MAC address.
host *src-MAC-addr* | *src-MAC-addr mask*	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.
host *dst-MAC-addr* | *dst-MAC-addr mask*	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.
type mask	(Optional) Specifies the EtherType number of a packet with Ethernet II or SNAP encapsulation to identify the protocol of the packet. • *type* is 0 to 65535, specified in hexadecimal. • *mask* is a mask of don't care bits applied to the EtherType before testing for a match.
aarp	(Optional) Specifies EtherType AppleTalk Address Resolution Protocol that maps a data-link address to a network address.
amber	(Optional) Specifies EtherType DEC-Amber.
appletalk	(Optional) Specifies EtherType AppleTalk/EtherTalk.
dec-spanning	(Optional) Specifies EtherType Digital Equipment Corporation (DEC) spanning tree.
decnet-iv	(Optional) Specifies EtherType DECnet Phase IV protocol.
diagnostic	(Optional) Specifies EtherType DEC-Diagnostic.

dsm	(Optional) Specifies EtherType DEC-DSM.
etype-6000	(Optional) Specifies EtherType 0x6000.
etype-8042	(Optional) Specifies EtherType 0x8042.
lat	(Optional) Specifies EtherType DEC-LAT.
lavc-sca	(Optional) Specifies EtherType DEC-LAVC-SCA.
lsap *lsap-number mask*	(Optional) Specifies the LSAP number (0 to 65535) of a packet with 802.2 encapsulation to identify the protocol of the packet. The *mask* is a mask of don't care bits applied to the LSAP number before testing for a match.
mop-console	(Optional) Specifies EtherType DEC-MOP Remote Console.
mop-dump	(Optional) Specifies EtherType DEC-MOP Dump.
msdos	(Optional) Specifies EtherType DEC-MSDOS.
mumps	(Optional) Specifies EtherType DEC-MUMPS.
netbios	(Optional) Specifies EtherType DEC- Network Basic Input/Output System (NetBIOS).
vines-echo	(Optional) Specifies EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems.
vines-ip	(Optional) Specifies EtherType VINES IP.
xns-idp	(Optional) Specifies EtherType Xerox Network Systems (XNS) protocol suite.
cos *cos*	(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 **cos** 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 3.3SE	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 2: 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

Examples

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.

```
Switch(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:

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

This example permits all packets with EtherType 0x4321:

```
Switch(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
deny	Denies from the MAC access-list configuration. Denies non-IP traffic to be forwarded if conditions are matched.
mac access-list extended	Creates an access list based on MAC addresses for non-IP traffic.
show access-lists	Displays access control lists configured on a switch.

protocol (IPv6 snooping)

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

protocol {**dhcp** | **ndp**}

no protocol {**dhcp** | **ndp**}

Syntax Description

dhcp	Specifies that addresses should be gleaned in Dynamic Host Configuration Protocol (DHCP) packets.
ndp	Specifies that addresses should be gleaned in Neighbor Discovery Protocol (NDP) packets.

Command Default

Snooping and recovery are attempted using both DHCP and NDP.

Command Modes

IPv6 snooping configuration mode

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

If an address does not match the prefix list associated with DHCP or NDP, then control packets will be dropped and recovery of the binding table entry will not be attempted with that protocol.

- Using the **no protocol** {**dhcp** | **ndp**} command indicates that a protocol will not be used for snooping or gleaning.
- If the **no protocol dhcp** command is used, DHCP can still be used for binding table recovery.
- Data glean can recover with DHCP and NDP, though destination guard will only recovery through DHCP.

Examples

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:

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

security level (IPv6 snooping)

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

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

Syntax Description

glean	Extracts addresses from the messages and installs them into the binding table without performing any verification.
guard	Performs both glean and inspect. Additionally, RA and DHCP server messages are rejected unless they are received on a trusted port or another policy authorizes them.
inspect	Validates messages for consistency and conformance; in particular, address ownership is enforced. Invalid messages are dropped.

Command Default

The default security level is guard.

Command Modes

IPv6 snooping configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Examples

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:

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

show aaa clients

To show AAA client statistics, use the **show aaa clients** command.

show aaa clients [**detailed**]

Syntax Description

detailed	(Optional) Shows detailed AAA client statistics.

Command Modes

User EXEC

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Examples

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

```
Switch# 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 3.3SE	This command was introduced.

Examples

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

```
Switch# 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

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

Command Modes

User EXEC

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Examples

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

```
Switch# 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

detailed	(Optional) Displays private AAA servers as seen by the AAA Server MIB.
public	(Optional) Displays public AAA servers as seen by the AAA Server MIB.
detailed	(Optional) Displays detailed AAA server statistics.

Command Modes

User EXEC

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Examples

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

```
Switch# 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 3.3SE	This command was introduced.

Examples

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

```
Switch# 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 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

database	(Optional) Shows only data stored in session database.
handle *handle-id*	(Optional) Specifies the particular handle for which Auth Manager information is to be displayed.
details	(Optional) Shows detailed information.
interface *type number*	(Optional) Specifies a particular interface type and number for which Auth Manager information is to be displayed.
mac *mac-address*	(Optional) Specifies the particular MAC address for which you want to display information.
method *method-name*	(Optional) Specifies the particular authentication method for which Auth Manager information is to be displayed. If you specify a method (**dot1x**, **mab**, or **webauth**), you may also specify an interface.
session-id *session-id*	(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 3.3SE	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 3: 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.
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 4: Authentication Method States

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

Examples

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

```
Switch# 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:

```
Switch# 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 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

clients	(Optional) Display CISP client details.
interface *interface-id*	(Optional) Display CISP information about the specified interface. Valid interfaces include physical ports and port channels.
registrations	Displays CISP registrations.
summary	(Optional) Displays CISP summary.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Examples

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

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

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

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

```
Gi3/0/23
```

Related Commands

Command	Description
cisp enable	Enable Client Information Signalling Protocol (CISP)
dot1x credentials *profile*	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

all	(Optional) Displays the IEEE 802.1x information for all interfaces.
count	(Optional) Displays total number of authorized and unauthorized clients.
details	(Optional) Displays the IEEE 802.1x interface details.
statistics	(Optional) Displays the IEEE 802.1x statistics for all interfaces.
summary	(Optional) Displays the IEEE 802.1x summary for all interfaces.
interface *type number*	(Optional) Displays the IEEE 802.1x status for the specified port.

Command Modes

User EXEC

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Examples

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

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

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

```
Switch# 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:

```
Switch# 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 3.3SE	This command was introduced.

Examples

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

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

Related Commands

Command	Description
clear eap sessions	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**]

Syntax Description

detail	(Optional) Displays detailed statistics information.

Command Modes

User EXEC

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

In a switch stack, all statistics are generated on the stack master. If a new active switch is elected, the statistics counters reset.

Examples

This is an example of output from the **show ip dhcp snooping statistics** command:

```
Switch> 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:

```
Switch> 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 5: DHCP Snooping Statistics

DHCP Snooping Statistic	Description
Packets Processed by DHCP Snooping	Total number of packets handled by DHCP snooping, including forwarded and dropped packets.
Packets Dropped Because IDB not known	Number of errors when the input interface of the packet cannot be determined.
Queue full	Number of errors when an internal queue used to process the packets is full. This might happen if DHCP packets are received at an excessively high rate and rate limiting is not enabled on the ingress ports.
Interface is in errdisabled	Number of times a packet was received on a port that has been marked as error disabled. This might happen if packets are in the processing queue when a port is put into the error-disabled state and those packets are subsequently processed.
Rate limit exceeded	Number of times the rate limit configured on the port was exceeded and the interface was put into the error-disabled state.
Received on untrusted ports	Number of times a DHCP server packet (OFFER, ACK, NAK, or LEASEQUERY) was received on an untrusted port and was dropped.
Nonzero giaddr	Number of times the relay agent address field (giaddr) in the DHCP packet received on an untrusted port was not zero, or the **no ip dhcp snooping information option allow-untrusted** 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 **ip dhcp snooping verify mac-address** 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.

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

show radius server-group

To display properties for the RADIUS server group, use the **show radius server-group** command.

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

Syntax Description

name	Name of the server group. The character string used to name the group of servers must be defined using **the aaa group server radius** command.
all	Displays properties for all of the server groups.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.3SE	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.

Examples

This is an example of output from the **show radius server-group all** command:

```
Switch# 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 6: 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.

Field	Description
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".
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

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

Command Modes

User EXEC

Command History

Release	Modification
Cisco IOS XE 3.3SE	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.

Examples

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.

```
Switch> 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.

```
Switch> 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 7: show storm-control Field Descriptions

Field	Description
Interface	Displays the ID of the interface.
Filter State	Displays the status of the filter: • Blocking—Storm control is enabled, and a storm has occurred. • Forwarding—Storm control is enabled, and no storms have occurred. • Inactive—Storm control is disabled.
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*]

Syntax Description

map-name	(Optional) Name of a specific VLAN access map.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Examples

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

```
Switch# show vlan access-map
Vlan access-map "vmap4"  10
  Match clauses:
    ip  address: al2
  Action:
    forward
Vlan access-map "vmap4"  20
  Match clauses:
    ip  address: al2
  Action:
    forward
```

show vlan group

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

show vlan group [**group-name** *vlan-group-name* **[user_count]**]

Syntax Description

group-name *vlan-group-name*	(Optional) Displays the VLANs mapped to the specified VLAN group.
user_count	(Optional) Displays the number of users in each VLAN mapped to a specified VLAN group.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.3SE	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.

Examples

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

```
Switch# show vlan group group-name group2
vlan group group1 :40-45
```

This example shows how to display number of users in each of the VLANs in a group:

```
Switch# show vlan group group-name group2 user_count
  VLAN     : Count
-------------------
  40         : 5
  41         : 8
  42         : 12
  43         : 2
  44         : 9
  45         : 0
```

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

action	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.
shutdown	Disables the port during a storm.
trap	Sends an SNMP trap when a storm occurs.
broadcast	Enables broadcast storm control on the interface.
multicast	Enables multicast storm control on the interface.
unicast	Enables unicast storm control on the interface.
level	Specifies the rising and falling suppression levels as a percentage of total bandwidth of the port.
level	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.
level-low	(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.
level bps	Specifies the rising and falling suppression levels as a rate in bits per second at which traffic is received on the port.
bps	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.
bps-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.
level pps	Specifies the rising and falling suppression levels as a rate in packets per second at which traffic is received on the port.

pps	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 3.3SE	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 (BDPU) 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.

Examples

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

```
Switch(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:

```
Switch(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:

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

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

```
Switch(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

static	Enables aging for statically configured secure addresses on this port.
time *time*	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.
type	Sets the aging type.
absolute	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.
inactivity	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 3.3SE	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.

Examples

This example sets the aging time as 2 hours for absolute aging for all the secure addresses on the port:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(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:

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# switchport port-security aging time 2
Switch(config-if)# switchport port-security aging type inactivity
Switch(config-if)# switchport port-security aging static
```

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

```
Switch(config)# interface gigabitethernet1/0/2
Switch(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 3.3SE	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.

Examples

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

```
Switch(config)# interface gigabitethernet 2/0/2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport port-security
Switch(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:

```
Switch(config)# interface gigabitethernet 2/0/2
Switch(config-if)# switchport port-security mac-address sticky
```

```
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.4141
Switch(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 3.3SE	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.

- 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.

Examples

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.

```
Switch(config)# interface gigabitethernet 2/0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(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

protect	Sets the security violation protect mode.
restrict	Sets the security violation restrict mode.
shutdown	Sets the security violation shutdown mode.
shutdown vlan	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 3.3SE	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.
- 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.

Examples

This example show how to configure a port to shut down only the VLAN if a MAC security violation occurs:

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

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

enable	Enables tracking.
reachable-lifetime	(Optional) Specifies the maximum amount of time a reachable entry is considered to be directly or indirectly reachable without proof of reachability. • The **reachable-lifetime** keyword can be used only with the **enable** keyword. • Use of the **reachable-lifetime** keyword overrides the global reachable lifetime configured by the **ipv6 neighbor binding reachable-lifetime** command.
value	Lifetime value, in seconds. The range is from 1 to 86400, and the default is 300.
infinite	Keeps an entry in a reachable or stale state for an infinite amount of time.
disable	Disables tracking.
stale-lifetime	(Optional) Keeps the time entry in a stale state, which overwrites the global stale-lifetime configuration. • The stale lifetime is 86,400 seconds. • The **stale-lifetime** keyword can be used only with the **disable** keyword. • Use of the **stale-lifetime** keyword overrides the global stale lifetime configured by the **ipv6 neighbor binding stale-lifetime** command.

Command Default

The time entry is kept in a reachable state.

Command Modes

IPv6 snooping configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	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.

Examples

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:

```
Switch(config)# ipv6 snooping policy policy1
Switch(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 3.3SE	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.

Examples

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:

```
Switch(config)# ipv6  nd inspection  policy1
Switch(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:

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

wireless dot11-padding

To enable over-the-air frame padding, use the **wireless dot11-padding** command. To disable, use the **no** form of the command.

wireless dot11-padding

no wireless dot11-padding

Command Default

Disabled.

Command Modes

config

Command History

Release	Modification
	This command was introduced.

Usage Guidelines

None.

Examples

This example shows how to enable over-the-air frame padding

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#wireless dot11-padding
```

wireless security dot1x

To configure IEEE 802.1x global configurations, use the **wireless security dot1x** command.

wireless security dot1x [**eapol-key** {**retries** *retries*| **timeout** *milliseconds*}| **group-key interval** *sec*| **identity-request** {**retries** *retries*| **timeout** *seconds*}| **radius [call-station-id]** {**ap-macaddress| ap-macaddress-ssid| ipaddress| macaddress**}| **request** {**retries** *retries*| **timeout** *seconds*}| **wep key** {**index 0**| **index 3**}]

Syntax Description

eapol-key	Configures eapol-key related parameters.
retries *retries*	(Optional) Specifies the maximum number of times (0 to 4 retries) that the controller retransmits an EAPOL (WPA) key message to a wireless client. The default value is 2.
timeout *milliseconds*	(Optional) Specifies the amount of time (200 to 5000 milliseconds) that the controller waits before retransmitting an EAPOL (WPA) key message to a wireless client using EAP or WPA/WPA-2 PSK. The default value is 1000 milliseconds.
group-key interval *sec*	Configures EAP-broadcast key renew interval time in seconds (120 to 86400 seconds).
identity-request	Configures EAP ID request related parameters.
retries *retries*	(Optional) Specifies the maximum number of times (0 to 4 retries) that the controller request the EAP ID. The default value is 2.
timeout *seconds*	(Optional) Specifies the amount of time (1 to 120 seconds) that the controller waits before retransmitting an EAP Identity Request message to a wireless client. The default value is 30 seconds.
radius	Configures radius messages.
call-station-id	(Optional) Configures Call-Station Id sent in radius messages.
ap-macaddress	Sets Call Station Id Type to the AP's MAC Address.
ap-macaddress-ssid	Sets Call Station Id Type to 'AP MAC address':'SSID'.
ipaddress	Sets Call Station Id Type to the system's IP Address.
macaddress	Sets Call Station Id Type to the system's MAC Address.
request	Configures EAP request related parameters.

retries *retries*	(Optional) For EAP messages other than Identity Requests or EAPOL (WPA) key messages, specifies the maximum number of times (0 to 20 retries) that the controller retransmits the message to a wireless client. The default value is 2.
timeout *seconds*	(Optional) For EAP messages other than Identity Requests or EAPOL (WPA) key messages, specifies the amount of time (1 to 120 seconds) that the controller waits before retransmitting the message to a wireless client. The default value is 30 seconds.
wep key	Configures 802.1x WEP related paramters.
index 0	Specifies the WEP key index value as 0
index 3	Specifies the WEP key index value as 3

Command Default

Default for eapol-key-timeout: 1 second.

Default for eapol-key-retries: 2 retries.

Command Modes

config

Command History

Release	Modification
	This command was introduced.

Usage Guidelines

None.

Examples

This example lists all the commands under **wireless security dot1x** .

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#wireless security dot1x ?
  eapol-key         Configure eapol-key related parameters
  group-key         Configures EAP-broadcast key renew interval time in seconds
  identity-request  Configure EAP ID request related parameters
  radius            Configure radius messages
  request           Configure EAP request related parameters
  wep               Configure 802.1x WEP related paramters
  <cr>
```

wireless security lsc

To configure locally significant certificates, use the **wireless security lsc** command.

wireless security lsc {**ap-provision** [**auth-list** *mac-addr*| **revert** *number*]| **other-params** *key-size*| **subject-params** *country state city orgn dept email*| **trustpoint** *trustpoint*}

Syntax Description

ap-provision	Specifies the access point provision list settings.
auth-list *mac-addr*	Specifies the provision list authorization settings.
revert *number*	Specifies the number of times the access point attempts to join the controller using an LSC before reverting to the default certificate. The maximum number of attempts cannot exceed 255.
other-params *key-size*	Specifies the device certificate key size settings.
subject-params *country state city orgn dept email*	Specifies the device certificate settings. Country, state, city, organization, department, and email of the certificate authority.
trustpoint *trustpoint*	Specifies the LSC Trustpoint.

Command Default

None

Command Modes

config

Command History

Release	Modification
	This command was introduced.

Usage Guidelines

You can configure only one CA server. To configure a different CA server, delete the configured CA server by using the config certificate lsc ca-server delete command, and then configure a different CA server.

If you configure an access point provision list, only the access points in the provision list are provisioned when you enable AP provisioning (in Step 8). If you do not configure an access point provision list, all access points with an MIC or SSC certificate that join the controller are LSC provisioned.

Examples

This example shows how to configure locally significant certificate:

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#wireless security lsc ?
  ap-provision    Provisioning the AP's with LSC's
```

```
other-params    Configure Other Parameters for Device Certs
subject-params  Configure the Subject Parameters for Device Certs
trustpoint      Configure LSC Trustpoint
<cr>
```

wireless security strong-password

To configure strong password enforcement options, use the **wireless security strong-password** command. To disable strong password, use the no form of the command.

wireless security strong-password

no wireless security strong-password

Command Default

None.

Command Modes

config

Command History

Release	Modification
	This command was introduced.

Usage Guidelines

None.

Examples

This example shows how to configure a strong-password for wireless security.

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#wireless security strong-password
```

wireless wps ap-authentication

To configure the access point neighbor authentication, use the **wireless wps ap-authentication** command. To remove the access point neighbor authentication, use the no form of the command.

wireless wps ap-authentication [**threshold** *value*]

no wireless wps ap-authentication [threshold]

Syntax Description

threshold *value*	Specifies that the WMM-enabled clients are on the wireless LAN. Threshold value (1 to 255).

Command Default

None.

Command Modes

config

Command History

Release	Modification
	This command was introduced.

Usage Guidelines

None.

Examples

This example shows how to set the threshold value for WMM-enabled clients.

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#wireless wps ap-authentication threshold 65
```

wireless wps auto-immune

To enable protection from denial of service (DoS) attacks, use the **wireless wps auto-immune** command. To disable, use the no form of the command.

wireless wps auto-immune

no wireless wps auto-immune

Command Default

Disabled.

Command Modes

config

Command History

Release	Modification
	This command was introduced.

Usage Guidelines

A potential attacker can use specially crafted packets to mislead the Intrusion Detection System (IDS) into treating a legitimate client as an attacker. It causes the controller to disconnect this legitimate client and launch a DoS attack. The auto-immune feature, when enabled, is designed to protect against such attacks. However, conversations using Cisco 792x phones might be interrupted intermittently when the auto-immune feature is enabled. If you experience frequent disruptions when using 792x phones, you might want to disable this feature.

Examples

This example shows how to enable protection from denial of service (DoS) attack:

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#wireless wps auto-immune
```

wireless wps cids-sensor

To configure Intrusion Detection System (IDS) sensors for the Wireless Protection System (WPS), use the **wireless wps cids-sensor** command. To remove the Intrusion Detection System (IDS) sensors for the Wireless Protection System (WPS), use the no form of the command.

wireless wps cids-sensor *index* [**ip-address** *ip-addr* **username** *username* **password** *password_type password*]

no wireless wps cids-sensor *index*

Syntax Description

index	Specifies the IDS sensor internal index.
ip-address *ip-addr* **username** *username* **password** *password_type password*	Specifies the IDS sensor IP address, IDS sensor username, password type and IDS sensor password.

Command Default

Disabled.

Command Modes

config

Command History

Release	Modification
	This command was introduced.

Usage Guidelines

None

Examples

This example shows how to configure the Intrusion Detection System with the IDS index, IDS sensor IP address, IDS username and IDS password.

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#wireless wps cids-sensor 1 10.0.0.51 Sensor_user0doc1 passowrd01
```

wireless wps client-exclusion

To configure client exclusion policies, use the **wireless wps client-exclusion** command. To remove the client exclusion policies, use the no form of the command.

wireless wps client-exclusion {**all**| **dot11-assoc**| **dot11-auth**| **dot1x-auth**| **ip-theft**| **web-auth**}

no wireless wps client-exclusion {**all**| **dot11-assoc**| **dot11-auth**| **dot1x-auth**| **ip-theft**| **web-auth**}

Syntax Description

dot11-assoc	Specifies that the controller excludes clients on the sixth 802.11 association attempt, after five consecutive failures.
dot11-auth	Specifies that the controller excludes clients on the sixth 802.11 authentication attempt, after five consecutive failures.
dot1x-auth	Specifies that the controller excludes clients on the sixth 802.11X authentication attempt, after five consecutive failures.
ip-theft	Specifies that the control excludes clients if the IP address is already assigned to another device.
web-auth	Specifies that the controller excludes clients on the fourth web authentication attempt, after three consecutive failures.
all	Specifies that the controller excludes clients for all of the above reasons.

Command Default

Enabled.

Command Modes

config

Command History

Release	Modification
	This command was introduced.

Usage Guidelines

None.

Examples

This example shows how to disable clients on the 802.11 association attempt after five consecutive failures.

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#wireless wps client-exclusion dot11-assoc
```

wireless wps mfp infrastructure

To configure Management Frame Protection (MFP), use the **wireless wps mfp infrastructure** command. To remove the Management Frame Protection (MFP), use the no form of the command.

wireless wps mfp infrastructure

no wireless wps mfp infrastructure

Command Default

None.

Command Modes

config

Command History

Release	Modification
	This command was introduced.

Usage Guidelines

None.

Examples

This example shows how to enable the infrastructure MFP.

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#wireless wps mfp infrastructure
```

wireless wps rogue

To configure various rouge parameters, use the **wireless wps rogue** command.

wireless wps rogue {**adhoc**| **client**} [**alert** *mac-addr*| **contain** *mac-addr no-of-aps*]

Syntax Description

adhoc	Configures the status of an Independent Basic Service Set (IBSS or ad-hoc) rogue access point.
client	Configures rogue clients
alert *mac-addr*	Generates an SNMP trap upon detection of the ad-hoc rogue, and generates an immediate alert to the system administrator for further action for the MAC address of the ad-hoc rogue access point.
contain *mac-addr no-of-aps*	Contains the offending device so that its signals no longer interfere with authorized clients. Maximum number of Cisco access points assigned to actively contain the ad-hoc rogue access point (1 through 4, inclusive).

Command Default

None.

Command Modes

Global configuration

Command History

Release	Modification
	This command was introduced.

Usage Guidelines

None.

Examples

This example shows how to generate an immediate alert to the system administrator for further action for the MAC address of the ad-hoc rogue access point.

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#wireless wps rouge adhoc alert mac_addr
```

wireless wps shun-list re-sync

To force the controller to synchronization with other controllers in the mobility group for the shun list, use the **wireless wps shun-list re-sync** command.

wireless wps shun-list re-sync

Command Default

None.

Command Modes

Any command mode

Command History

Release	Modification
	This command was introduced.

Usage Guidelines

None.

Examples

This example shows how to configure the controller to synchronize with other controllers for the shun list.

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#wireless wps shun-list re-sync
```

vlan access-map

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

vlan access-map *name* [*number*]

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

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

Syntax Description

name	Name of the VLAN map.
number	(Optional) The sequence number of the map entry that you want to create or modify (0 to 65535). If you are creating a VLAN map and the sequence number is not specified, it is automatically assigned in increments of 10, starting from 10. This number is the sequence to insert to, or delete from, a VLAN access-map entry.

Command Default

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

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	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.

Examples

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.

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

This example shows how to delete VLAN map vac1:

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

vlan filter

To apply a VLAN map to one or more VLANs, use the **vlan filter** command in global configuration mode on the switch stack or on a standalone switch. To remove the map, use the **no** form of this command.

vlan filter *mapname* **vlan-list** {*list*| **all**}

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

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

Syntax Description

mapname	Name of the VLAN map entry.
vlan-list	Specifies which VLANs to apply the map to.
list	The list of one or more VLANs in the form tt, uu-vv, xx, yy-zz, where spaces around commas and dashes are optional. The range is 1 to 4094.
all	Adds the map to all VLANs.

Command Default

There are no VLAN filters.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	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.

Examples

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

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

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

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

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

vlan group

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

vlan group *group-name* **vlan-list** *vlan-list*

no vlan group *group-name* **vlan-list** *vlan-list*

Syntax Description

group-name	Name of the VLAN group. The group name may contain up to 32 characters and must begin with a letter.
vlan-list *vlan-list*	Specifies one or more VLANs to be added to the VLAN group. The *vlan-list* argument can be a single VLAN ID, a list of VLAN IDs, or VLAN ID range. Multiple entries are separated by a hyphen (-) or a comma (,).

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

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

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

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

Examples

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

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

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

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