D Commands

dot1x max-reauth-req

To change the maximum number of times that the Cisco NX-OS device retransmits reauthentication requests to supplicants on an interface before the session times out, use the **dot1x max-reauth-req** command. To revert to the default, use the **no** form of this command.

dot1x max-reauth-req *retry-count*

no dot1x max-reauth-req

Syntax Description

retry-count	Retry count for reauthentication requests. The range is from 1 to 10.

Command Default

2 retries

Command Modes

Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must use the **feature dot1x** command before you configure 802.1X.

This command does not require a license.

Examples

This example shows how to change the maximum number of reauthorization request retries for an interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# dot1x max-reauth-req 3
```

This example shows how to revert to the default maximum number of reauthorization request retries for an interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# no dot1x max-reauth-req
```

Related Commands

Command	Description
feature dot1x	Enables the 802.1X feature.

Command	Description
show dot1x all	Displays all 802.1X information.

dot1x max-req

To change the maximum number of requests that the Cisco NX-OS device sends to a supplicant before restarting the 802.1X authentication, use the **dot1x max-req** command. To revert to the default, use the **no** form of this command.

dot1x max-req *retry-count*

no dot1x max-req

Syntax Description

retry-count	Retry count for request sent to supplicant before restarting 802.1X reauthentication. The range is from 1 to 10.

Command Default

Global configuration: 2 retries

Interface configuration: Global configuration setting

Command Modes

Global configuration Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must use the **feature dot1x** command before you configure 802.1X.

This command does not require a license.

Examples

This example shows how to change the maximum number of request retries for the global 802.1X configuration:

```
switch# configure terminal
switch(config)# dot1x max-req 3
```

This example shows how to revert to the default maximum number of request retries for the global 802.1X configuration:

```
switch# configure terminal
switch(config)# no dot1x max-req
```

This example shows how to change the maximum number of request retries for an interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# dot1x max-req 4
```

This example shows how to revert to the default maximum number of request retries for an interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# no dot1x max-req
```

Related Commands

Command	Description
feature dot1x	Enables the 802.1X feature.
show dot1x all	Displays all 802.1X information.

dot1x pae authenticator

To create the 802.1X authenticator port access entity (PAE) role for an interface, use the **dot1x pae authenticator** command. To remove the 802.1X authenticator PAE role, use the **no** form of this command.

dot1x pae authenticator

no dot1x pae authenticator

Syntax Description

This command has no arguments or keywords.

Command Default

802.1X automatically creates the authenticator PAE when you enable the feature on an interface.

Command Modes

Interface configuration

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

You must use the **feature dot1x** command before you configure 802.1X.

When you enable 802.1X on an interface, the Cisco NX-OS software creates an authenticator port access entity (PAE) instance. An authenticator PAE is a protocol entity that supports authentication on the interface. When you disable 802.1X on the interface, the Cisco NX-OS software does not automatically clear the authenticator PAE instances. You can explicitly remove the authenticator PAE from the interface and then reapply it, as needed.

This command does not require a license.

Examples

This example shows how to create the 802.1X authenticator PAE role on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/4
switch(config-if)# dot1x pae authenticator
```

This example shows how to remove the 802.1X authenticator PAE role from an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/4
switch(config-if)# no dot1x pae authenticator
```

Related Commands

Command	Description
feature dot1x	Enables the 802.1X feature.

Command	Description
show dot1x interface	Displays 802.1X feature status information for an interface.

dot1x port-control

To control the 802.1X authentication performed on an interface, use the **dot1x port-control** command. To revert to the default, use the **no** form of this command.

dot1x port-control {**auto**| **force-authorized**| **force-unauthorized**}

no dot1x port-control {**auto**| **force-authorized**| **force-unauthorized**}

Syntax Description

auto	Enables 802.1X authentication on the interface.
force-authorized	Disables 802.1X authentication on the interface and allows all traffic on the interface without authentication.
force-unauthorized	Disallows all authentication on the interface.

Command Default

force-authorized

Command Modes

Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must use the **feature dot1x** command before you configure 802.1X.

This command does not require a license.

Examples

This example shows how to change the 802.1X authentication action performed on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# dot1x port-control auto
```

This example shows how to revert to the default 802.1X authentication action performed on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# dot1x port-control auto
```

Related Commands

Command	Description
feature dot1x	Enables the 802.1X feature.
show dot1x interface ethernet	Displays 802.1X information for an interface.

dot1x radius-accounting

To enable RADIUS accounting for 802.1X, use the **dot1x radius-accounting** command. To revert to the default, use the **no** form of this command.

dot1x radius-accounting

no dot1x radius-accounting

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must use the **feature dot1x** command before you configure 802.1X.

This command does not require a license.

Examples

This example shows how to enable RADIUS accounting for 802.1X authentication:

```
switch# configure terminal
switch(config)# dot1x radius-accounting
```

This example shows how to disable RADIUS accounting for 802.1X authentication:

```
switch# configure terminal
switch(config)# no dot1x radius-accounting
```

Related Commands

Command	Description
feature dot1x	Enables the 802.1X feature.
show running-config dot1x all	Displays all 802.1X information in the running configuration.

dot1x re-authentication (EXEC)

To manually reauthenticate 802.1X supplicants, use the **dot1x re-authentication** command.

dot1x reauthentication [**interface ethernet** *slot* | *port*]

Syntax Description

interface ethernet *slot*/*port*	(Optional) Specifies the interface for manual reauthentication.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must use the **feature dot1x** command before you configure 802.1X.

This command does not require a license.

Examples

This example shows how to reauthenticate 802.1X supplicants manually:

```
switch# dot1x re-authentication
```

This example shows how to reauthenticate the 802.1X supplicant on an interface manually:

```
switch# dot1x re-authentication interface ethernet 2/1
```

Related Commands

Command	Description
feature dot1x	Enables the 802.1X feature.
show dot1x all	Displays all 802.1X information.

dot1x re-authentication (global configuration and interface configuration)

To enable periodic reauthenticate of 802.1X supplicants, use the **dot1x re-authentication** command. To revert to the default, use the **no** form of this command.

dot1x re-authentication

no dot1x re-authentication

Syntax Description

This command has no arguments or keywords.

Command Default

Global configuration: Disabled

Interface configuration: Global configuration setting

Command Modes

Global configurationInterface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must use the **feature dot1x** command before you configure 802.1X.

In global configuration mode, this command configures periodic reauthentication for all supplicants on the Cisco NX-OS device. In interface configuration mode, this command configures periodic reauthentication only for supplicants on the interface.

This command does not require a license.

Examples

This example shows how to enable periodic reauthentication of 802.1X supplicants:

```
switch# configure terminal
switch(config)# dot1x re-authentication
```

This example shows how to disable periodic reauthentication of 802.1X supplicants:

```
switch# configure terminal
switch(config)# no dot1x re-authentication
```

This example shows how to enable periodic reauthentication of 802.1X supplicants on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# dot1x re-authentication
```

This example shows how to disable periodic reauthentication of 802.1X supplicants on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# no dot1x re-authentication
```

Related Commands

Command	Description
feature dot1x	Enables the 802.1X feature.
show dot1x all	Displays all 802.1X information.

dot1x system-auth-control

To enable 802.1X authentication, use the **dot1x system-auth-control** command. To disable 802.1X authentication, use the **no** form of this command.

dot1x system-auth-control

no dot1x system-auth-control

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The **dot1x system-auth-control** command does not delete the 802.1X configuration.

You must use the **feature dot1x** command before you configure 802.1X.

This command does not require a license.

Examples

This example shows how to disable 802.1X authentication:

```
switch# configure terminal
switch(config)# no dot1x system-auth-control
```

This example shows how to enable 802.1X authentication:

```
switch# configure terminal
switch(config)# dot1x system-auth-control
```

Related Commands

Command	Description
feature dot1x	Enables the 802.1X feature.
show dot1x	Displays 802.1X feature status information.

dot1x timeout quiet-period

To configure the 802.1X quiet-period timeout globally or for an interface, use the **dot1x timeout quiet-period** command. To revert to the default, use the **no** form of this command.

dot1x timeout quiet-period *seconds*

no dot1x timeout quiet-period

Syntax Description

seconds	Number of seconds for the 802.1X quiet-period timeout. The range is from 1 to 65535.

Command Default

Global configuration: 60 seconds

Interface configuration: The value of the global configuration

Command Modes

Global configuration Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The 802.1X quiet-period timeout is the number of seconds that the device remains in the quiet state following a failed authentication exchange with a supplicant.

You must use the **feature dot1x** command before you configure 802.1X.

Note You should change the default value only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain supplicants and authentication servers.

This command does not require a license.

Examples

This example shows how to configure the global 802.1X quiet-period timeout:

```
switch# configure terminal
switch(config)# dot1x timeout quiet-period 45
```

This example shows how to revert to the default global 802.1X quiet-period timeout:

```
switch# configure terminal
switch(config)# no dot1x timeout quiet-period
```

This example shows how to configure the 802.1X quiet-period timeout for an interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# dot1x timeout quiet-period 50
```

This example shows how to revert to the default 802.1X quiet-period timeout for an interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# no dot1x timeout quiet-period
```

Related Commands

Command	Description
feature dot1x	Enables the 802.1X feature.
show dot1x all	Displays all 802.1X information.

dot1x timeout ratelimit-period

To configure the 802.1X rate-limit period timeout for the supplicants on an interface, use the **dot1x timeout ratelimit-period** command. To revert to the default, use the **no** form of this command.

dot1x timeout ratelimit-period *seconds*

no dot1x timeout ratelimit-period

Syntax Description

seconds	Number of seconds for the 802.1X rate-limit period timeout. The range is from 1 to 65535.

Command Default

0 seconds

Command Modes

Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The 802.1X rate-limit timeout period is the number of seconds that the authenticator ignores EAPOL-Start packets from supplicants that have successfully authenticated. This value overrides the global quiet period timeout.

You must use the **feature dot1x** command before you configure 802.1X.

Note You should change the default value only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain supplicants and authentication servers.

This command does not require a license.

Examples

This example shows how to configure the 802.1X rate-limit period timeout on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# dot1x timeout ratelimit-period 60
```

This example shows how to revert to the default 802.1X rate-limit period timeout on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# dot1x timeout ratelimit-period 60
```

Related Commands

Command	Description
feature dot1x	Enables the 802.1X feature.
show dot1x interface ethernet	Displays 802.1X information for an interface.

dot1x timeout re-authperiod

To configure the 802.1X reauthentication-period timeout either globally or on an interface, use the **dot1x timeout re-authperiod** command. To revert to the default, use the **no** form of this command.

dot1x timeout re-authperiod *seconds*

no dot1x timeout re-authperiod

Syntax Description

seconds	Number of seconds for the 802.1X reauthentication-period timeout. The range is from 1 to 65535.

Command Default

Global configuration: 3600 seconds

Interface configuration: Global configuration setting

Command Modes

Global configuration Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The 802.1X reauthentication timeout period is the number of seconds between reauthentication attempts.

You must use the **feature dot1x** command before you configure 802.1X.

Note You should change the default value only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain supplicants and authentication servers.

This command does not require a license.

Examples

This example shows how to configure the global 802.1X reauthentication-period timeout:

```
switch# configure terminal
switch(config)# dot1x timeout re-authperiod 3000
```

This example shows how to configure the 802.1X reauthentication-period timeout on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# dot1x timeout re-authperiod 3300
```

Related Commands

Command	Description
feature dot1x	Enables the 802.1X feature.
show dot1x all	Displays all 802.1X information.

dot1x timeout server-timeout

To configure the 802.1X server timeout for an interface, use the **dot1x timeout server-timeout** command. To revert to the default, use the **no** form of this command.

dot1x timeout server-timeout *seconds*

no dot1x timeout server-timeout

Syntax Description

seconds	Number of seconds for the 802.1X server timeout. The range is from 1 to 65535.

Command Default

30 seconds

Command Modes

Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The 802.1X server timeout for an interface is the number of seconds that the Cisco NX-OS device waits before retransmitting a packet to the authentication server. This value overrides the global reauthentication period timeout.

You must use the **feature dot1x** command before you configure 802.1X.

Note You should change the default value only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain supplicants and authentication servers.

This command does not require a license.

Examples

This example shows how to configure the global 802.1X server timeout interval:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# dot1x timeout server-timeout 45
```

This example shows how to revert to the default global 802.1X server timeout interval:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# dot1x timeout server-timeout 45
```

Related Commands

Command	Description
feature dot1x	Enables the 802.1X feature.
show dot1x interface ethernet	Displays 802.1X information for an interface.

dot1x timeout supp-timeout

To configure the 802.1X supplicant timeout for an interface, use the **dot1x timeout supp-timeout** command. To revert to the default, use the **no** form of this command.

dot1x timeout supp-timeout *seconds*

no dot1x timeout supp-timeout

Syntax Description

seconds	Number of seconds for the 802.1X supplicant timeout. The range is from 1 to 65535.

Command Default

30 seconds

Command Modes

Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The 802.1X supplicant timeout for an interface is the number of seconds that the Cisco NX-OS device waits for the supplicant to respond to an EAP request frame before the Cisco NX-OS device retransmits the frame.

You must use the **feature dot1x** command before you configure 802.1X.

Note You should change the default value only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain supplicants and authentication servers.

This command does not require a license.

Examples

This example shows how to configure the 802.1X server timeout interval on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# dot1x timeout supp-timeout 45
```

This example shows how to revert to the default 802.1X server timeout interval on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# no dot1x timeout supp-timeout
```

Related Commands

Command	Description
feature dot1x	Enables the 802.1X feature.
show dot1x interface ethernet	Displays 802.1X information for an interface.

dot1x timeout tx-period

To configure the 802.1X transmission-period timeout either globally or for an interface, use the **dot1x timeout tx-period** command. To revert to the default, use the **no** form of this command.

dot1x timeout tx-period *seconds*

no dot1x timeout tx-period

Syntax Description

seconds	Number of seconds for the 802.1X transmission-period timeout. The range is from 1 to 65535.

Command Default

Global configuration: 60 seconds

Interface configuration: Global configuration setting

Command Modes

Global configuration Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The 802.1X transmission-timeout period is the number of seconds that the Cisco NX-OS device waits for a response to an EAP-request/identity frame from the supplicant before retransmitting the request.

You must use the **feature dot1x** command before you configure 802.1X.

Note You should change the default value only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain supplicants and authentication servers.

This command does not require a license.

Examples

This example shows how to configure the global 802.1X transmission-period timeout:

```
switch# configure terminal
switch(config)# dot1x timeout tx-period 45
```

This example shows how to revert to the default global 802.1X transmission-period timeout:

```
switch# configure terminal
switch(config)# no dot1x timeout tx-period
```

This example shows how to configure the 802.1X transmission-period timeout for an interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# dot1x timeout tx-period 45
```

This example shows how to revert to the default 802.1X transmission-period timeout for an interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# no dot1x timeout tx-period
```

Related Commands

Command	Description
feature dot1x	Enables the 802.1X feature.
show dot1x all	Displays all 802.1X information.

deadtime

To configure the dead-time interval for a RADIUS or TACACS+ server group, use the **deadtime** command. To revert to the default, use the **no** form of this command.

deadtime *minutes*

no deadtime *minutes*

Syntax Description

minutes	Number of minutes for the interval. The range is from 0 to 1440 minutes. **Note** Setting the dead-time interval to 0 disables the timer.

Command Default

0 minutes

Command Modes

RADlUS server group configuration TACACS+ server group configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must use the **feature tacacs+** command before you configure TACACS+.

This command does not require a license.

Examples

This example shows how to set the dead-time interval to 2 minutes for a RADIUS server group:

```
switch# configure terminal
switch(config)# aaa group server radius RadServer
switch(config-radius)# deadtime 2
```

This example shows how to set the dead-time interval to 5 minutes for a TACACS+ server group:

```
switch# configure terminal
switch(config)# feature tacacs+
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# deadtime 5
```

This example shows how to revert to the dead-time interval default:

```
switch# configure terminal
switch(config)# feature tacacs+
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# no deadtime 5
```

Related Commands

Command	Description
aaa group server	Configures AAA server groups.
radius-server host	Configures a RADIUS server.
show radius-server groups	Displays RADIUS server group information.
show tacacs-server groups	Displays TACACS+ server group information.
feature tacacs+	Enables TACACS+.
tacacs-server host	Configures a TACACS+ server.

delete ca-certificate

To delete certificate authority certificates, use the **delete ca-certificate** command.

delete ca-certificate

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Trustpoint configuration

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

This command deletes the CA certificate or certificate chain corresponding to the trustpoint CA. As a result, the trustpoint CA is no longer trusted. If there is an identity certificate form the CA, you must delete it before you can delete the CA certificate. This prevents the accidental deletion of a CA certificate when you have not yet deleted the identity certificate obtained from that CA. Deleting the CA certificate may be necessary when you no longer want to trust the CA because the CA is compromised or the CA certificate has expired.

The trustpoint configuration, certificates, and key pair configurations are persistent only after saving to the startup configuration. Deletions become persistent only after you save the running configuration to the startup configuration.

Enter the **copy running-config startup-config** command to make the certificate and key pair deletions persistent.

This command does not require a license.

Examples

This example shows how to delete a certificate authority certificate:

```
switch# configure terminal
switch(config)# crypto ca trustpoint admin-ca
switch(config-trustpoint)# delete ca-certificate
```

Related Commands

Command	Description
delete certificate	Deletes the identity certificate.
delete crl	Deletes the CRL from the trustpoint.

delete certificate

To delete the identity certificate, use the **delete certificate** command.

delete certificate [force]

Syntax Description

force	(Optional) Forces the deletion of the identity certificate.

Command Default

None

Command Modes

Trustpoint configuration

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

Use the **delete certificate** command to delete the identity certificate obtained from the trustpoint CA when the identity certificate expires or the corresponding key pair is compromised. Applications on the device are left without any identity certificate to use after you delete the last or the only identity certificate present. The Cisco NX-OS software generates an error message if the certificate being deleted is the only certificate present or is the last identity certificate in a chain. You can use the optional **force** keyword to remove the certificate.

The trustpoint configuration, certificates, and key pair configurations are persistent only after saving to the startup configuration. Deletions become persistent only after you save the running configuration to the startup configuration.

Enter the **copy running-config startup-config** command to make the certificate and key pair deletions persistent.

This command does not require a license.

Examples

This example shows how to delete the identity certificate:

```
switch# configure terminal
switch(config)# crypto ca trustpoint admin-ca
switch(config-trustpoint)# delete certificate
```

This example shows how to force the deletion of the identity certificate:

```
switch# configure terminal
switch(config)# crypto ca trustpoint admin-ca
switch(config-trustpoint)# delete certificate force
```

Related Commands

Command	Description
delete ca-certificate	Deletes the certificate authority certificate.
delete crl	Deletes the CRL from the trustpoint.

delete crl

To delete the certificate revocation list (CRL) from the trustpoint, use the **delete crl** command.

delete crl

Syntax Description

This command has no argument or keywords.

Command Default

None

Command Modes

Trustpoint configuration

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to delete the CRL from the trustpoint:

```
switch# configure terminal
switch(config)# crypto ca trustpoint admin-ca
switch(config-trustpoint)# delete crl
```

Related Commands

Command	Description
delete ca-certificate	Deletes the certificate authority certificate.
delete certificate	Deletes the identity certificate.

deny (ARP)

To create an ARP ACL rule that denies ARP traffic that matches its conditions, use the **deny** command. To remove a rule, use the **no** form of this command.

General Syntax

[*sequence-number*] **deny ip** {**any**| **host** *sender-IP*| *sender-IP sender-IP-mask*} **mac** {**any**| **host** *sender-MAC*| *sender-MAC sender-MAC-mask*} **[log]**

[*sequence-number*] **deny request ip** {**any**| **host** *sender-IP*| *sender-IP sender-IP-mask*} **mac** {**any**| **host** *sender-MAC*| *sender-MAC sender-MAC-mask*} **[log]**

[*sequence-number*] **deny response ip** {**any**| **host** *sender-IP*| *sender-IP sender-IP-mask*} {**any**| **host** *target-IP*| *target-IP target-IP-mask*} **mac** {**any**| **host** *sender-MAC*| *sender-MAC sender-MAC-mask*} [**any**| **host** *target-MAC*| *target-MAC target-MAC-mask*] **[log]**

no *sequence-number*

no deny ip {**any**| **host** *sender-IP*| *sender-IP sender-IP-mask*} **mac** {**any**| **host** *sender-MAC*| *sender-MAC sender-MAC-mask*} **[log]**

no deny request ip {**any**| **host** *sender-IP*| *sender-IP sender-IP-mask*} **mac** {**any**| **host** *sender-MAC*| *sender-MAC sender-MAC-mask*} **[log]**

no deny response ip {**any**| **host** *sender-IP*| *sender-IP sender-IP-mask*} {**any**| **host** *target-IP*| *target-IP target-IP-mask*} **mac** {**any**| **host** *sender-MAC*| *sender-MAC sender-MAC-mask*} [**any**| **host** *target-MAC*| *target-MAC target-MAC-mask*] **[log]**

Syntax Description

sequence-number	(Optional) Sequence number of the **deny** command, which causes the device to insert the command in that numbered position in the access list. Sequence numbers maintain the order of rules within an ACL. A sequence number can be any integer between 1 and 4294967295. By default, the first rule in an ACL has a sequence number of 10. If you do not specify a sequence number, the device adds the rule to the end of the ACL and assigns a sequence number that is 10 greater than the sequence number of the preceding rule. Use the **resequence** command to reassign sequence numbers to rules.
ip	Introduces the IP address portion of the rule.

any	(Optional) Specifies that any host matches the part of the rule that contains the **any** keyword. You can use the **any** to specify the sender IP address, target IP address, sender MAC address, and target MAC address.
host *sender-IP*	(Optional) Specifies that the rule matches ARP packets only when the sender IP address in the packet matches the value of the *sender-IP* argument. Valid values for the *sender-IP* argument are IPv4 addresses in dotted-decimal format.
sender-IP sender-IP-mask	(Optional) IPv4 address and mask for the set of IPv4 addresses that the sender IP address in the packet can match. The *sender-IP* and *sender-IP-mask* argument must be given in dotted-decimal format. Specifying 255.255.255.255 as the *sender-IP-mask* argument is the equivalent of using the **host** keyword.
mac	Introduces the MAC address portion of the rule.
host *sender-MAC*	(Optional) Specifies that the rule matches ARP packets only when the sender MAC address in the packet matches the value of the *sender-MAC* argument. Valid values for the *sender-MAC* argument are MAC addresses in dotted-hexadecimal format.
sender-MAC sender-MAC-mask	(Optional) MAC address and mask for the set of MAC addresses that the sender MAC address in the packet can match. The *sender-MAC* and *sender-MAC-mask* argument must be given in dotted-hexadecimal format. Specifying ffff.ffff.ffff as the *sender-MAC-mask* argument is the equivalent of using the **host** keyword.
log	(Optional) Specifies that the device logs ARP packets that match the rule.
request	(Optional) Specifies that the rule applies only to packets containing ARP request messages. **Note** If you omit both the **request** and the **response** keywords, the rule applies to all ARP messages.
response	(Optional) Specifies that the rule applies only to packets containing ARP response messages. **Note** If you omit both the **request** and the **response** keywords, the rule applies to all ARP messages.

host *target-IP*	(Optional) Specifies that the rule matches ARP packets only when the target IP address in the packet matches the value of the *target-IP* argument. You can specify **host** *target-IP* only when you use the **response** keyword. Valid values for the *target-IP* argument are IPv4 addresses in dotted-decimal format.
target-IP target-IP-mask	(Optional) IPv4 address and mask for the set of IPv4 addresses that the target IP address in the packet can match. You can specify *target-IP target-IP-mask* only when you use the **response** keyword. The *target-IP* and *target-IP-mask* argument must be given in dotted-decimal format. Specifying 255.255.255.255 as the *target-IP-mask* argument is the equivalent of using the **host** keyword.
host *target-MAC*	(Optional) Specifies that the rule matches ARP packets only when the target MAC address in the packet matches the value of the *target-MAC* argument. You can specify **host** *target-MAC* only when you use the **response** keyword. Valid values for the *target-MAC* argument are MAC addresses in dotted-hexadecimal format.
target-MAC target-MAC-mask	(Optional) MAC address and mask for the set of MAC addresses that the target MAC address in the packet can match. You can specify *target-MAC target-MAC-mask* only when you use the **response** keyword. The *target-MAC* and *target-MAC-mask* argument must be given in dotted-hexadecimal format. Specifying ffff.ffff.ffff as the *target-MAC-mask* argument is the equivalent of using the **host** keyword.

Command Default

None

Command Modes

ARP ACL configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

A newly created ARP ACL contains no rules.

If you do not specify a sequence number, the device assigns to the rule a sequence number that is 10 greater than the last rule in the ACL.

When the device applies an ARP ACL to a packet, it evaluates the packet with every rule in the ACL. The device enforces the first rule that has conditions that are satisfied by the packet. When the conditions of more than one rule are satisfied, the device enforces the rule with the lowest sequence number.

If you do not specify either the **response** or **request** keyword, the rule applies to packets that contain any ARP message.

This command does not require a license.

Examples

This example shows how to enter ARP access list configuration mode for an ARP ACL named arp-acl-01 and add a rule that denies ARP request messages that contain a sender IP address that is within the 10.32.143.0 subnet:

```
switch# conf t
switch(config)# arp access-list arp-acl-01
switch(config-arp-acl)# deny request ip 10.32.143.0 255.255.255.0 mac any
```

Related Commands

Command	Description
arp access-list	Configures an ARP ACL.
ip arp inspection filter	Applies an ARP ACL to a VLAN.
permit (ARP)	Configures a permit rule in an ARP ACL.
remark	Configures a remark in an ACL.
show arp access-list	Displays all ARP ACLs or one ARP ACL.

deny (IPv4)

To create an IPv4 ACL rule that denies traffic matching its conditions, use the **deny** command. To remove a rule, use the **no** form of this command.

General Syntax

[*sequence-number*] **deny** *protocol source destination* [**dscp** *dscp*| **precedence** *precedence*] **[fragments] [log]** [**time-range** *time-range-name*] [**packet-length** *operator packet-length* [*packet-length*]]

no deny *protocol source destination* [**dscp** *dscp*| **precedence** *precedence*] **[fragments] [log]** [**time-range** *time-range-name*] [**packet-length** *operator packet-length* [*packet-length*]]

no *sequence-number*

Internet Control Message Protocol

[*sequence-number*] **deny icmp** *source destination* [*icmp-message*| *icmp-type* [*icmp-code*]] [**dscp** *dscp*| **precedence** *precedence*] **[fragments] [log]** [**time-range** *time-range-name*] [**packet-length** *operator packet-length* [*packet-length*]]

Internet Group Management Protocol

[*sequence-number*] **deny igmp** *source destination* [*igmp-message*] [**dscp** *dscp*| **precedence** *precedence*] **[fragments] [log]** [**time-range** *time-range-name*] [**packet-length** *operator packet-length* [*packet-length*]]

Internet Protocol v4

[*sequence-number*] **deny ip** *source destination* [**dscp** *dscp*| **precedence** *precedence*] **[fragments] [log]** [**time-range** *time-range-name*] [**packet-length** *operator packet-length* [*packet-length*]]

Transmission Control Protocol

[*sequence-number*] **deny tcp** *source* [*operator port* [*port*]| **portgroup** *portgroup*] *destination* [*operator port* [*port*]| **portgroup** *portgroup*] [**dscp** *dscp*| **precedence** *precedence*] **[fragments] [log]** [**time-range** *time-range-name*] [*flags*] **[established]** [**packet-length** *operator packet-length* [*packet-length*]]

User Datagram Protocol

[*sequence-number*] **deny udp** *source* [*operator port* [*port*]| **portgroup** *portgroup*] *destination* [*operator port* [*port*]| **portgroup** *portgroup*] [**dscp** *dscp*| **precedence** *precedence*] **[fragments] [log]** [**time-range** *time-range-name*] [**packet-length** *operator packet-length* [*packet-length*]]

Syntax Description

sequence-number	(Optional) Sequence number of the **deny** command, which causes the device to insert the command in that numbered position in the access list. Sequence numbers maintain the order of rules within an ACL. A sequence number can be any integer between 1 and 4294967295. By default, the first rule in an ACL has a sequence number of 10. If you do not specify a sequence number, the device adds the rule to the end of the ACL and assigns a sequence number that is 10 greater than the sequence number of the preceding rule. Use the **resequence** command to reassign sequence numbers to rules.
protocol	Name or number of the protocol of packets that the rule matches. For details about the methods that you can use to specify this argument, see “Protocol” in the “Usage Guidelines” section.
source	Source IPv4 addresses that the rule matches. For details about the methods that you can use to specify this argument, see “Source and Destination” in the “Usage Guidelines” section.
destination	Destination IPv4 addresses that the rule matches. For details about the methods that you can use to specify this argument, see “Source and Destination” in the “Usage Guidelines” section.

dscp *dscp*	

(Optional) Specifies that the rule matches only those packets with the specified 6-bit differentiated services value in the DSCP field of the IP header. The *dscp* argument can be one of the following numbers or keywords:

- 0–63—The decimal equivalent of the 6 bits of the DSCP field. For example, if you specify 10, the rule matches only those packets that have the following bits in the DSCP field: 001010.
- **af11**—Assured Forwarding (AF) class 1, low drop probability (001010)
- **af12**—AF class 1, medium drop probability (001100)
- **af13**—AF class 1, high drop probability (001110)
- **af21**—AF class 2, low drop probability (010010)
- **af22**—AF class 2, medium drop probability (010100)
- **af23**—AF class 2, high drop probability (010110)
- **af31**—AF class 3, low drop probability (011010)
- **af32**—AF class 3, medium drop probability (011100)
- **af33**—AF class 3, high drop probability (011110)
- **af41**—AF class 4, low drop probability (100010)
- **af42**—AF class 4, medium drop probability (100100)
- **af43**—AF class 4, high drop probability (100110)
- **cs1**—Class-selector (CS) 1, precedence 1 (001000)
- **cs2**—CS2, precedence 2 (010000)
- **cs3**—CS3, precedence 3 (011000)
- **cs4**—CS4, precedence 4 (100000)
- **cs5**—CS5, precedence 5 (101000)
- **cs6**—CS6, precedence 6 (110000)

	• **cs7—**CS7, precedence 7 (111000) • **default—**Default DSCP value (000000) • **ef—**Expedited Forwarding (101110)
precedence *precedence*	(Optional) Specifies that the rule matches only packets that have an IP Precedence field with the value specified by the *precedence* argument. The *precedence* argument can be a number or a keyword, as follows: • 0–7—Decimal equivalent of the 3 bits of the IP Precedence field. For example, if you specify 3, the rule matches only packets that have the following bits in the DSCP field: 011. • **critical—**Precedence 5 (101) • **flash—**Precedence 3 (011) • **flash-override—**Precedence 4 (100) • **immediate—**Precedence 2 (010) • **internet—**Precedence 6 (110) • **network—**Precedence 7 (111) • **priority—**Precedence 1 (001) • **routine—**Precedence 0 (000)
fragments	(Optional) Specifies that the rule matches only those packets that are noninitial fragments. You cannot specify this keyword in the same rule that you specify Layer 4 options, such as a TCP port number, because the information that the devices requires to evaluate those options is contained only in initial fragments.
log	(Optional) Specifies that the device generates an informational logging message about each packet that matches the rule. The message includes the following information: • Whether the protocol was TCP, UDP, ICMP or a number • Source and destination addresses • Source and destination port numbers, if applicable

time-range *time-range-name*	(Optional) Specifies the time range that applies to this rule. You can configure a time range by using the **time-range** command. The *time-range-name* argument can be up to 64 alphanumeric, case-sensitive characters.
icmp-message	(ICMP only: Optional) ICMP message type that the rule matches. This argument can be an integer from 0 to 255 or one of the keywords listed under “ICMP Message Types” in the “Usage Guidelines” section.
icmp-type [*icmp-code*]	(ICMP only: Optional) ICMP message type that the rule matches. Valid values for the *icmp-type* argument are an integer from 0 to 255. If the ICMP message type supports message codes, you can use the *icmp-code* argument to specify the code that the rule matches. For more information about ICMP message types and codes, see http://www.iana.org/assignments/icmp-parameters .
igmp-message	(IGMP only: Optional) IGMP message type that the rule matches. The *igmp-message* argument can be the IGMP message number, which is an integer from 0 to 15. It can also be one of the following keywords: • **dvmrp—**Distance Vector Multicast Routing Protocol • **host-query—**Host query • **host-report—**Host report • **pim—**Protocol Independent Multicast • **trace—**Multicast trace

operator port [*port*]	(Optional; TCP and UDP only) Rule matches only packets that are from a source port or sent to a destination port that satisfies the conditions of the *operator* and *port* arguments. Whether these arguments apply to a source port or a destination port depends upon whether you specify them after the *source* argument or after the *destination* argument. The *port* argument can be the name or the number of a TCP or UDP port. Valid numbers are integers from 0 to 65535. For listings of valid port names, see "TCP Port Names" and "UDP Port Names" in the "Usage Guidelines" section. A second *port* argument is required only when the *operator* argument is a range. The *operator* argument must be one of the following keywords: • **eq—**Matches only if the port in the packet is equal to the *port* argument. • **gt—**Matches only if the port in the packet is greater than and not equal to the *port* argument. • **lt—**Matches only if the port in the packet is less than and not equal to the *port* argument. • **neq—**Matches only if the port in the packet is not equal to the *port* argument. • **range—**Requires two *port* arguments and matches only if the port in the packet is equal to or greater than the first *port* argument and equal to or less than the second *port* argument.
portgroup *portgroup*	(Optional; TCP and UDP only) Specifies that the rule matches only packets that are from a source port or to a destination port that is a member of the IP port object group specified by the *portgroup* argument, which can be up to 64 alphanumeric, case-sensitive characters. Whether the IP port object group applies to a source port or a destination port depends upon whether you specify it after the *source* argument or after the *destination* argument. Use the **object-group ip port** command to create and change IP port object groups.

flags	(TCP only; Optional) TCP control bit flags that the rule matches. The value of the *flags* argument must be one or more of the following keywords: • **ack** • **fin** • **psh** • **rst** • **syn** • **urg**
established	(TCP only; Optional) Specifies that the rule matches only packets that belong to an established TCP connection. The device considers TCP packets with the ACK or RST bits set to belong to an established connection.
packet-length*operatorpacket-length* [*packet-length*	(Optional) Rule matches only packets that have a length in bytes that satisfies the condition specified by the *operator* and *packet-length* arguments. Valid values for the *packet-length* argument are whole numbers from 20 to 9210. The *operator* argument must be one of the following keywords: • **eq—**Matches only if the packet length in bytes is equal to the *packet-length* argument. • **gt—**Matches only if the packet length in bytes is greater than the *packet-length* argument. • **lt—**Matches only if the packet length in bytes is less than the *packet-length* argument. • **neq—**Matches only if the packet length in bytes is not equal to the *packet-length* argument. • **range—**Requires two *packet-length* arguments and matches only if the packet length in bytes is equal to or greater than the first *packet-length* argument and equal to or less than the second *packet-length* argument.

Command Default

A newly created IPv4 ACL contains no rules.

If you do not specify a sequence number, the device assigns the rule a sequence number that is 10 greater than the last rule in the ACL.

Command Modes IPv4 ACL configuration

Command History

Release	Modification
4.1(2)	Support was added for the following: • The **ahp**, **eigrp**, **esp**, **gre**, **nos**, **ospf**, **pcp**, and **pim** protocol keywords. • The **packet-length** keyword.
4.0(1)	This command was introduced.

Usage Guidelines When the device applies an IPv4 ACL to a packet, it evaluates the packet with every rule in the ACL. The device enforces the first rule that has conditions that are satisfied by the packet. When the conditions of more than one rule are satisfied, the device enforces the rule with the lowest sequence number.

This command does not require a license.

Protocol

You can specify the protocol of packets that the rule applies to by the protocol name or the number of the protocol. If you want the rule to apply to all IPv4 traffic, use the **ip** keyword.

The protocol keyword that you specify affects the additional keywords and arguments that are available. Unless otherwise specified, only the other keywords that apply to all IPv4 protocols are available. Those keywords include the following:

- ◦ **dscp**
  ◦ **fragments**
  ◦ **log**
  ◦ **packet-length**
  ◦ **precedence**
  ◦ **time-range**

Valid protocol numbers are from 0 to 255.

Valid protocol names are the following keywords:

- **ahp—**Specifies that the rule applies to authentication header protocol (AHP) traffic only.
- **eigrp—**Specifies that the rule applies to Enhanced Interior Gateway Routing Protocol (EIGRP) traffic only.
- **esp—**Specifies that the rule applies to Encapsulating Security Protocol (ESP) traffic only.
- **gre—**Specifies that the rule applies to General Routing Encapsulation (GRE) traffic only.

- **icmp—**Specifies that the rule applies to ICMP traffic only. When you use this keyword, the *icmp-message* argument is available, in addition to the keywords that are available for all valid values of the *protocol* argument.
- **igmp—**Specifies that the rule applies to IGMP traffic only. When you use this keyword, the *igmp-type* argument is available, in addition to the keywords that are available for all valid values of the *protocol* argument.
- **ip—**Specifies that the rule applies to all IPv4 traffic.
- **nos—**Specifies that the rule applies to KA9Q NOS-compatible IP-over-IP tunneling traffic only.
- **ospf—**Specifies that the rule applies to Open Shortest Path First (OSPF) traffic only.
- **pcp—**Specifies that the rule applies to payload compression protocol (PCP) traffic only.
- **pim—**Specifies that the rule applies to protocol-independent multicast (PIM) traffic only.
- **tcp—**Specifies that the rule applies to TCP traffic only. When you use this keyword, the *flags* and *operator* arguments and the **portgroup** and **established** keywords are available, in addition to the keywords that are available for all valid values of the *protocol* argument.
- **udp—**Specifies that the rule applies to UDP traffic only. When you use this keyword, the *operator* argument and the **portgroup** keyword are available, in addition to the keywords that are available for all valid values of the *protocol* argument.

Source and Destination

You can specify the *source* and *destination* arguments in one of several ways. In each rule, the method that you use to specify one of these arguments does not affect how you specify the other argument. When you configure a rule, use the following methods to specify the *source* and *destination* arguments:

- IP address group object—You can use an IPv4 address group object to specify a *source* or *destination* argument. Use the **object-group ip address** command to create and change IPv4 address group objects. The syntax is as follows:

```
addrgroup
```

```
address-group-name
```

The following example shows how to use an IPv4 address object group named lab-gateway-svrs to specify the *destination* argument:

```
switch(config-acl)# deny ip any addrgroup lab-gateway-svrs
```

- Address and network wildcard—You can use an IPv4 address followed by a network wildcard to specify a host or a network as a source or destination. The syntax is as follows:

```
IPv4-address network-wildcard
```

The following example shows how to specify the *source* argument with the IPv4 address and network wildcard for the 192.168.67.0 subnet:

```
switch(config-acl)# deny tcp 192.168.67.0 0.0.0.255 any
```

- Address and variable-length subnet mask—You can use an IPv4 address followed by a variable-length subnet mask (VLSM) to specify a host or a network as a source or destination. The syntax is as follows:

```
IPv4-address/prefix-len
```

The following example shows how to specify the *source* argument with the IPv4 address and VLSM for the 192.168.67.0 subnet:

```
switch(config-acl)# deny udp 192.168.67.0/24 any
```

- Host address—You can use the **host** keyword and an IPv4 address to specify a host as a source or destination. The syntax is as follows:

```
host
IPv4-address
```

This syntax is equivalent to *IPv4-address*/32 and *IPv4-address* 0.0.0.0.

The following example shows how to specify the *source* argument with the **host** keyword and the 192.168.67.132 IPv4 address:

```
switch(config-acl)# deny icmp host 192.168.67.132 any
```

- Any address—You can use the **any** keyword to specify that a source or destination is any IPv4 address. For examples of the use of the **any** keyword, see the examples in this section. Each example shows how to specify a source or destination by using the **any** keyword.

ICMP Message Types

The *icmp-message* argument can be one of the following keywords:

- **administratively-prohibited**—Administratively prohibited
- **alternate-address**—Alternate address
- **conversion-error**—Datagram conversion
- **dod-host-prohibited**—Host prohibited
- **dod-net-prohibited**—Net prohibited
- **echo**—Echo (ping)
- **echo-reply**—Echo reply
- **general-parameter-problem**—Parameter problem
- **host-isolated**—Host isolated
- **host-precedence-unreachable**—Host unreachable for precedence
- **host-redirect**—Host redirect
- **host-tos-redirect**—Host redirect for ToS
- **host-tos-unreachable**—Host unreachable for ToS
- **host-unknown**—Host unknown
- **host-unreachable**—Host unreachable
- **information-reply**—Information replies

- **information-request—**Information requests
- **mask-reply—**Mask replies
- **mask-request—**Mask requests
- **mobile-redirect—**Mobile host redirect
- **net-redirect—**Network redirect
- **net-tos-redirect—**Net redirect for ToS
- **net-tos-unreachable—**Network unreachable for ToS
- **net-unreachable—**Net unreachable
- **network-unknown—**Network unknown
- **no-room-for-option—**Parameter required but no room
- **option-missing—**Parameter required but not present
- **packet-too-big—**Fragmentation needed and DF set
- **parameter-problem—**All parameter problems
- **port-unreachable—**Port unreachable
- **precedence-unreachable—**Precedence cutoff
- **protocol-unreachable—**Protocol unreachable
- **reassembly-timeout—**Reassembly timeout
- **redirect—**All redirects
- **router-advertisement—**Router discovery advertisements
- **router-solicitation—**Router discovery solicitations
- **source-quench—**Source quenches
- **source-route-failed—**Source route failed
- **time-exceeded—**All time-exceeded messages
- **timestamp-reply—**Time-stamp replies
- **timestamp-request—**Time-stamp requests
- **traceroute—**Traceroute
- **ttl-exceeded—**TTL exceeded
- **unreachable—**All unreachables

TCP Port Names

When you specify the *protocol* argument as **tcp**, the *port* argument can be a TCP port number, which is an integer from 0 to 65535. It can also be one of the following keywords:

bgp—Border Gateway Protocol (179)

chargen—Character generator (19)

cmd—Remote commands (rcmd, 514)

daytime—Daytime (13)

discard—Discard (9)

domain—Domain Name Service (53)

drip—Dynamic Routing Information Protocol (3949)

echo—Echo (7)

exec—EXEC (rsh, 512)

finger—Finger (79)

ftp—File Transfer Protocol (21)

ftp-data—FTP data connections (20)

gopher—Gopher (7)

hostname—NIC hostname server (11)

ident—Ident Protocol (113)

irc—Internet Relay Chat (194)

klogin—Kerberos login (543)

kshell—Kerberos shell (544)

login—Login (rlogin, 513)

lpd—Printer service (515)

nntp—Network News Transport Protocol (119)

pim-auto-rp—PIM Auto-RP (496)

pop2—Post Office Protocol v2 (19)

pop3—Post Office Protocol v3 (11)

smtp—Simple Mail Transport Protocol (25)

sunrpc—Sun Remote Procedure Call (111)

tacacs—TAC Access Control System (49)

talk—Talk (517)

telnet—Telnet (23)

time—Time (37)

uucp—UNIX-to-UNIX Copy Program (54)

whois—WHOIS/NICNAME (43)

www—World Wide Web (HTTP, 80)

UDP Port Names

When you specify the *protocol* argument as **udp**, the *port* argument can be a UDP port number, which is an integer from 0 to 65535. It can also be one of the following keywords:

biff—Biff (mail notification, comsat, 512)

bootpc—Bootstrap Protocol (BOOTP) client (68)

bootps—Bootstrap Protocol (BOOTP) server (67)

discard—Discard (9)

dnsix—DNSIX security protocol auditing (195)

domain—Domain Name Service (DNS, 53)

echo—Echo (7)

isakmp—Internet Security Association and Key Management Protocol (5)

mobile-ip—Mobile IP registration (434)

nameserver—IEN116 name service (obsolete, 42)

netbios-dgm—NetBIOS datagram service (138)

netbios-ns—NetBIOS name service (137)

netbios-ss—NetBIOS session service (139)

non500-isakmp—Internet Security Association and Key Management Protocol (45)

ntp—Network Time Protocol (123)

pim-auto-rp—PIM Auto-RP (496)

rip—Routing Information Protocol (router, in.routed, 52)

snmp—Simple Network Management Protocol (161)

snmptrap—SNMP Traps (162)

sunrpc—Sun Remote Procedure Call (111)

syslog—System Logger (514)

tacacs—TAC Access Control System (49)

talk—Talk (517)

tftp—Trivial File Transfer Protocol (69)

time—Time (37)

who—Who service (rwho, 513)

xdmcp—X Display Manager Control Protocol (177)

Examples

This example shows how to configure an IPv4 ACL named acl-lab-01 with rules that deny all TCP and UDP traffic from the 10.23.0.0 and 192.168.37.0 networks to the 10.176.0.0 network and a final rule that permits all other IPv4 traffic:

```
switch# configure terminal
switch(config)# ip access-list acl-lab-01
switch(config-acl)# deny tcp 10.23.0.0/16 10.176.0.0/16
switch(config-acl)# deny udp 10.23.0.0/16 10.176.0.0/16
switch(config-acl)# deny tcp 192.168.37.0/16 10.176.0.0/16
switch(config-acl)# deny udp 192.168.37.0/16 10.176.0.0/16
switch(config-acl)# permit ip any any
```

This example shows how to configure an IPv4 ACL named acl-eng-to-marketing with a rule that denies all IP traffic from an IPv4 address object group named eng_workstations to an IP address object group named marketing_group followed by a rule that permits all other IPv4 traffic:

```
switch# configure terminal
switch(config)# ip access-list acl-eng-to-marketing
switch(config-acl)# deny ip addrgroup eng_workstations addrgroup marketing_group
switch(config-acl)# permit ip any any
```

Related Commands

Command	Description
fragments	Configures how an IP ACL processes noninitial fragments.
ip access-list	Configures an IPv4 ACL.
object-group ip address	Configures an IPv4 address object group.
object-group ip port	Configures an IP port object group.
permit (IPv4)	Configures a permit rule in an IPv4 ACL.
remark	Configures a remark in an IPv4 ACL.
show ip access-list	Displays all IPv4 ACLs or one IPv4 ACL.
statistics per-entry	Enables collection of statistics for each entry in an ACL.
time-range	Configures a time range.

deny (IPv6)

To create an IPv6 ACL rule that denies traffic matching its conditions, use the **deny** command. To remove a rule, use the **no** form of this command.

General Syntax

[*sequence-number*] **deny** *protocol source destination* [**dscp** *dscp*] [**flow-label** *flow-label-value*] **[fragments] [log]** [**time-range** *time-range-name*] [**packet-length** *operator packet-length* [*packet-length*]]

no deny *protocol source destination* [**dscp** *dscp*] [**flow-label** *flow-label-value*] **[fragments] [log]** [**time-range** *time-range-name*] [**packet-length** *operator packet-length* [*packet-length*]]

no *sequence-number*

Internet Control Message Protocol

[*sequence-number*| **no**] **deny icmp** *source destination* [*icmp-message*| *icmp-type* [*icmp-code*]] [**dscp** *dscp*] [**flow-label** *flow-label-value*] **[fragments] [log]** [**time-range** *time-range-name*] [**packet-length** *operator packet-length* [*packet-length*]]

Internet Protocol v6

[*sequence-number*] **deny ipv6** *source destination* [**dscp** *dscp*] [**flow-label** *flow-label-value*] **[fragments] [log]** [**time-range** *time-range-name*] [**packet-length** *operator packet-length* [*packet-length*]]

Stream Control Transmission Protocol

[*sequence-number*| **no**] **deny sctp** *source* [*operator port* [*port*]| **portgroup** *portgroup*] *destination* [*operator port* [*port*]| **portgroup** *portgroup*] [**dscp** *dscp*] [**flow-label** *flow-label-value*] **[fragments] [log]** [**time-range** *time-range-name*] [**packet-length** *operator packet-length* [*packet-length*]]

Transmission Control Protocol

[*sequence-number*] **deny tcp** *source* [*operator port* [*port*]| **portgroup** *portgroup*] *destination* [*operator port* [*port*]| **portgroup** *portgroup*] [**dscp** *dscp*] [**flow-label** *flow-label-value*] **[fragments] [log]** [**time-range** *time-range-name*] [*flags*] **[established]** [**packet-length** *operator packet-length* [*packet-length*]]

User Datagram Protocol

[*sequence-number*| **no**] **deny udp** *source* [*operator port* [*port*]| **portgroup** *portgroup*] *destination* [*operator port* [*port*]| **portgroup** *portgroup*] [**dscp** *dscp*] [**flow-label** *flow-label-value*] **[fragments] [log]** [**time-range** *time-range-name*] [**packet-length** *operator packet-length* [*packet-length*]]

Syntax Description

sequence-number	(Optional) Sequence number of the deny command, which causes the device to insert the command in that numbered position in the access list. Sequence numbers maintain the order of rules within an ACL. A sequence number can be any integer between 1 and 4294967295. By default, the first rule in an ACL has a sequence number of 10. If you do not specify a sequence number, the device adds the rule to the end of the ACL and assigns a sequence number that is 10 greater than the sequence number of the preceding rule. Use the **resequence** command to reassign sequence numbers to rules.

protocol	

Name or number of the protocol of packets that the rule matches. Valid numbers are from 0 to 255. Valid protocol names are the following keywords:

- **ahp—**Specifies that the rule applies to Authentication Header Protocol (AHP) traffic only. When you use this keyword, only the other keywords and arguments that apply to all IPv6 protocols are available.
- **esp—**Specifies that the rule applies to Encapsulating Security Payload (ESP) traffic only. When you use this keyword, only the other keywords and arguments that apply to all IPv6 protocols are available.
- **icmp—**Specifies that the rule applies to ICMP traffic only. When you use this keyword, the *icmp-message* argument is available, in addition to the keywords that are available for all valid values of the *protocol* argument.
- **ipv6—**Specifies that the rule applies to all IPv6 traffic. When you use this keyword, only the other keywords and arguments that apply to all IPv6 protocols are available.
- **pcp—**Specifies that the rule applies to Payload Compression Protocol (PCP) traffic only. When you use this keyword, only the other keywords and arguments that apply to all IPv6 protocols are available.
- **sctp—**Specifies that the rule applies to Stream Control Transmission Protocol (SCTP) traffic only. When you use this keyword, the *operator* argument and the **portgroup** keyword are available, in addition to the keywords that are available for all valid values of the *protocol* argument.
- **tcp—**Specifies that the rule applies to TCP traffic only. When you use this keyword, the *flags* and *operator* arguments and the **portgroup** and **established** keywords are available, in addition to the keywords that are available for all valid values of the *protocol* argument.
- **udp—**Specifies that the rule applies to UDP traffic only. When you use this keyword, the *operator* argument and the **portgroup** keyword are available, in addition to the keywords that are available for all valid values of the *protocol*

	argument.
source	Source IPv6 addresses that the rule matches. For details about the methods that you can use to specify this argument, see “Source and Destination” in the “Usage Guidelines” section.
destination	Destination IPv6 addresses that the rule matches. For details about the methods that you can use to specify this argument, see “Source and Destination” in the “Usage Guidelines” section.

dscp *dscp*	

(Optional) Specifies that the rule matches only packets with the specified 6-bit differentiated services value in the DSCP field of the IPv6 header. The *dscp* argument can be one of the following numbers or keywords:

- 0–63—The decimal equivalent of the 6 bits of the DSCP field. For example, if you specify 10, the rule matches only packets that have the following bits in the DSCP field: 001010.
- **af11**—Assured Forwarding (AF) class 1, low drop probability (001010)
- **af12**—AF class 1, medium drop probability (001100)
- **af13**—AF class 1, high drop probability (001110)
- **af21**—AF class 2, low drop probability (010010)
- **af22**—AF class 2, medium drop probability (010100)
- **af23**—AF class 2, high drop probability (010110)
- **af31**—AF class 3, low drop probability (011010)
- **af32**—AF class 3, medium drop probability (011100)
- **af33**—AF class 3, high drop probability (011110)
- **af41**—AF class 4, low drop probability (100010)
- **af42**—AF class 4, medium drop probability (100100)
- **af43**—AF class 4, high drop probability (100110)
- **cs1**—Class-selector (CS) 1, precedence 1 (001000)
- **cs2**—CS2, precedence 2 (010000)
- **cs3**—CS3, precedence 3 (011000)
- **cs4**—CS4, precedence 4 (100000)
- **cs5**—CS5, precedence 5 (101000)
- **cs6**—CS6, precedence 6 (110000)

	• **cs7—**CS7, precedence 7 (111000) • **default—**Default DSCP value (000000) • **ef—**Expedited Forwarding (101110)
flow-label *flow-label-value*	(Optional) Specifies that the rule matches only IPv6 packets whose Flow Label header field has the value specified by the *flow-label-value* argument. The *flow-label-value* argument can be an integer from 0 to 1048575.
fragments	(Optional) Specifies that the rule matches noninitial fragmented packets only. The device considers noninitial fragmented packets to be packets with a fragment extension header that contains a fragment offset that is not equal to zero. You cannot specify this keyword in the same rule that you specify Layer 4 options, such as a TCP port number, because the information that the devices requires to evaluate those options is contained only in initial fragments.
log	(Optional) Specifies that the device generates an informational logging message about each packet that matches the rule. The message includes the following information: • ACL name • Whether the packet was permitted or denied • Whether the protocol was TCP, UDP, ICMP or a number • Source and destination addresses and, if applicable, source and destination port numbers
time-range *time-range-name*	(Optional) Specifies the time range that applies to this rule. You can configure a time range by using the **time-range** command.
icmp-message	(ICMP only: Optional) ICMPv6 message type that the rule matches. This argument can be an integer from 0 to 255 or one of the keywords listed under “ICMPv6 Message Types” in the “Usage Guidelines” section.

icmp-type [*icmp-code*]	(ICMP only: Optional) ICMP message type that the rule matches. Valid values for the *icmp-type* argument are an integer from 0 to 255. If the ICMP message type supports message codes, you can use the *icmp-code* argument to specify the code that the rule matches. For more information about ICMP message types and codes, see http://www.iana.org/assignments/icmp-parameters .
operator port [*port*]	(Optional; TCP, UDP, and SCTP only) Rule matches only packets that are from a source port or sent to a destination port that satisfies the conditions of the *operator* and *port* arguments. Whether these arguments apply to a source port or a destination port depends upon whether you specify them after the *source* argument or after the *destination* argument. The *port* argument can be the name or the number of a TCP or UDP port. Valid numbers are integers from 0 to 65535. For listings of valid port names, see “TCP Port Names” and “UDP Port Names” in the “Usage Guidelines” section. A second *port* argument is required only when the *operator* argument is a range. The *operator* argument must be one of the following keywords: • **eq**—Matches only if the port in the packet is equal to the *port* argument. • **gt**—Matches only if the port in the packet is greater than and not equal to the *port* argument. • **lt**—Matches only if the port in the packet is less than and not equal to the *port* argument. • **neq**—Matches only if the port in the packet is not equal to the *port* argument. • **range**—Requires two *port* arguments and matches only if the port in the packet is equal to or greater than the first *port* argument and equal to or less than the second *port* argument.

portgroup *portgroup*	(Optional; TCP, UDP, and SCTP only) Specifies that the rule matches only packets that are from a source port or to a destination port that is a member of the IP port-group object specified by the *portgroup* argument. Whether the port-group object applies to a source port or a destination port depends upon whether you specify it after the *source* argument or after the *destination* argument. Use the **object-group ip port** command to create and change IP port-group objects.
established	(TCP only; Optional) Specifies that the rule matches only packets that belong to an established TCP connection. The device considers TCP packets with the ACK or RST bits set to belong to an established connection.
flags	(TCP only; Optional) Rule matches only packets that have specific TCP control bit flags set. The value of the *flags* argument must be one or more of the following keywords: • **ack** • **fin** • **psh** • **rst** • **syn** • **urg**

packet-length*operatorpacket-length* [*packet-length*	(Optional) Rule matches only packets that have a length in bytes that satisfies the condition specified by the *operator* and *packet-length* arguments. Valid values for the *packet-length* argument are whole numbers from 20 to 9210. The *operator* argument must be one of the following keywords: • **eq—**Matches only if the packet length in bytes is equal to the *packet-length* argument. • **gt—**Matches only if the packet length in bytes is greater than the *packet-length* argument. • **lt—**Matches only if the packet length in bytes is less than the *packet-length* argument. • **neq—**Matches only if the packet length in bytes is not equal to the *packet-length* argument. • **range—**Requires two *packet-length* arguments and matches only if the packet length in bytes is equal to or greater than the first *packet-length* argument and equal to or less than the second *packet-length* argument.

Command Default

None

Command Modes

IPv6 ACL configuration

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

A newly created IPv6 ACL contains no rules.

When the device applies an IPv6 ACL to a packet, it evaluates the packet with every rule in the ACL. The device enforces the first rule whose conditions are satisfied by the packet. When the conditions of more than one rule are satisfied, the device enforces the rule with the lowest sequence number.

This command does not require a license.

Source and Destination

You can specify the *source* and *destination* arguments in one of several ways. In each rule, the method you use to specify one of these arguments does not affect how you specify the other. When you configure a rule, use the following methods to specify the *source* and *destination* arguments:

- IPv6 address group object—You can use an IPv6 address group object to specify a *source* or *destination* argument. Use the **object-group ipv6 address** command to create and change IPv6 address group objects. The syntax is as follows:

addrgroup

address-group-name

The following example shows how to use an IPv6 address object group named lab-svrs-1301 to specify the *destination* argument:

```
switch(config-acl)# deny ipv6 any addrgroup lab-svrs-1301
```

- Address and variable-length subnet mask—You can use an IPv6 address followed by a variable-length subnet mask (VLSM) to specify a host or a network as a source or destination. The syntax is as follows:

IPv6-address/prefix-len

The following example shows how to specify the *source* argument with the IPv6 address and VLSM for the 2001:0db8:85a3:: network:

```
switch(config-acl)# deny udp 2001:0db8:85a3::/48 any
```

- Host address—You can use the **host** keyword and an IPv6 address to specify a host as a source or destination. The syntax is as follows:

host
IPv6-address

This syntax is equivalent to *IPv6-address*/128.

The following example shows how to specify the *source* argument with the **host** keyword and the 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 IPv6 address:

```
switch(config-acl)# deny icmp host 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 any
```

- Any address—You can use the **any** keyword to specify that a source or destination is any IPv6 address. For examples of the use of the **any** keyword, see the examples in this section. Each example shows how to specify a source or destination by using the **any** keyword.

ICMPv6 Message Types

The *icmp-message* argument can be one of the following keywords:

- **beyond-scope**—Destination beyond scope
- **destination-unreachable**—Destination address is unreachable
- **echo-reply**—Echo reply
- **echo-request**—Echo request (ping)
- **header**—Parameter header problems
- **hop-limit**—Hop limit exceeded in transit
- **mld-query**—Multicast Listener Discovery Query
- **mld-reduction**—Multicast Listener Discovery Reduction

- **mld-report—**Multicast Listener Discovery Report
- **nd-na—**Neighbor discovery neighbor advertisements
- **nd-ns—**Neighbor discovery neighbor solicitations
- **next-header—**Parameter next header problems
- **no-admin—**Administration prohibited destination
- **no-route—**No route to destination
- **packet-too-big—**Packet too big
- **parameter-option—**Parameter option problems
- **parameter-problem—**All parameter problems
- **port-unreachable—**Port unreachable
- **reassembly-timeout—**Reassembly timeout
- **redirect—**Neighbor redirect
- **renum-command—**Router renumbering command
- **renum-result—**Router renumbering result
- **renum-seq-number—**Router renumbering sequence number reset
- **router-advertisement—**Neighbor discovery router advertisements
- **router-renumbering—**All router renumbering
- **router-solicitation—**Neighbor discovery router solicitations
- **time-exceeded—**All time exceeded messages
- **unreachable—**All unreachable

TCP Port Names

When you specify the *protocol* argument as **tcp**, the *port* argument can be a TCP port number, which is an integer from 0 to 65535. It can also be one of the following keywords:

bgp—Border Gateway Protocol (179)

chargen—Character generator (19)

cmd—Remote commands (rcmd, 514)

daytime—Daytime (13)

discard—Discard (9)

domain—Domain Name Service (53)

drip—Dynamic Routing Information Protocol (3949)

echo—Echo (7)

exec—Exec (rsh, 512)

finger—Finger (79)

ftp—File Transfer Protocol (21)

ftp-data—FTP data connections (20)

gopher—Gopher (7)

hostname—NIC hostname server (11)

ident—Ident Protocol (113)

irc—Internet Relay Chat (194)

klogin—Kerberos login (543)

kshell—Kerberos shell (544)

login—Login (rlogin, 513)

lpd—Printer service (515)

nntp—Network News Transport Protocol (119)

pim-auto-rp—PIM Auto-RP (496)

pop2—Post Office Protocol v2 (19)

pop3—Post Office Protocol v3 (11)

smtp—Simple Mail Transport Protocol (25)

sunrpc—Sun Remote Procedure Call (111)

tacacs—TAC Access Control System (49)

talk—Talk (517)

telnet—Telnet (23)

time—Time (37)

uucp—Unix-to-Unix Copy Program (54)

whois—WHOIS/NICNAME (43)

www—World Wide Web (HTTP, 80)

UDP Port Names

When you specify the *protocol* argument as **udp**, the *port* argument can be a UDP port number, which is an integer from 0 to 65535. It can also be one of the following keywords:

biff—Biff (mail notification, comsat, 512)

bootpc—Bootstrap Protocol (BOOTP) client (68)

bootps—Bootstrap Protocol (BOOTP) server (67)

discard—Discard (9)

dnsix—DNSIX security protocol auditing (195)

domain—Domain Name Service (DNS, 53)

echo—Echo (7)

isakmp—Internet Security Association and Key Management Protocol (5)

mobile-ip—Mobile IP registration (434)

nameserver—IEN116 name service (obsolete, 42)

netbios-dgm—NetBIOS datagram service (138)

netbios-ns—NetBIOS name service (137)

netbios-ss—NetBIOS session service (139)

non500-isakmp—Internet Security Association and Key Management Protocol (45)

ntp—Network Time Protocol (123)

pim-auto-rp—PIM Auto-RP (496)

rip—Routing Information Protocol (router, in.routed, 52)

snmp—Simple Network Management Protocol (161)

snmptrap—SNMP Traps (162)

sunrpc—Sun Remote Procedure Call (111)

syslog—System Logger (514)

tacacs—TAC Access Control System (49)

talk—Talk (517)

tftp—Trivial File Transfer Protocol (69)

time—Time (37)

who—Who service (rwho, 513)

xdmcp—X Display Manager Control Protocol (177)

Examples

This example shows how to configure an IPv6 ACL named acl-lab13-ipv6 with rules denying all TCP and UDP traffic from the 2001:0db8:85a3:: and 2001:0db8:69f2:: networks to the 2001:0db8:be03:2112:: network:

```
switch# config t
switch(config)# ipv6 access-list acl-lab13-ipv6
switch(config-ipv6-acl)# deny tcp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
switch(config-ipv6-acl)# deny udp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
switch(config-ipv6-acl)# deny tcp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
switch(config-ipv6-acl)# deny udp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
```

This example shows how to configure an IPv6 ACL named ipv6-eng-to-marketing with a rule that denies all IPv6 traffic from an IPv6-address object group named eng_ipv6 to an IPv6-address object group named marketing_group:

```
switch# config t
switch(config)# ipv6 access-list ipv6-eng-to-marketing
switch(config-ipv6-acl)# deny ipv6 addrgroup eng_ipv6 addrgroup marketing_group
```

Related Commands

Command	Description
fragments	Configures how an IP ACL processes noninitial fragments.
ipv6 access-list	Configures an IPv6 ACL.
object-group ipv6 address	Configures an IPv6-address object group.
object-group ip port	Configures an IP-port object group.

Command	Description
permit (IPv6)	Configures a permit rule in an IPv6 ACL.
remark	Configures a remark in an ACL.
show ipv6 access-list	Displays all IPv6 ACLs or one IPv6 ACL.
statistics per-entry	Enables collection of statistics for each entry in an ACL.
time-range	Configures a time range.

deny (MAC)

To create a MAC access control list (ACL)+ rule that denies traffic matching its conditions, use the **deny** command. To remove a rule, use the **no** form of this command.

[*sequence-number*] **deny** *source destination* [*protocol*] [**cos** *cos-value*] [**vlan** *VLAN-ID*] [**time-range** *time-range-name*]

no deny *source destination* [*protocol*] [**cos** *cos-value*] [**vlan** *VLAN-ID*] [**time-range** *time-range-name*]

no *sequence-number*

Syntax Description

sequence-number	(Optional) Sequence number of the **deny** command, which causes the device to insert the command in that numbered position in the access list. Sequence numbers maintain the order of rules within an ACL. A sequence number can be any integer between 1 and 4294967295. By default, the first rule in an ACL has a sequence number of 10. If you do not specify a sequence number, the device adds the rule to the end of the ACL and assigns a sequence number that is 10 greater than the sequence number of the preceding rule. Use the **resequence** command to reassign sequence numbers to rules.
source	Source MAC addresses that the rule matches. For details about the methods that you can use to specify this argument, see “Source and Destination” in the “Usage Guidelines” section.
destination	Destination MAC addresses that the rule matches. For details about the methods that you can use to specify this argument, see “Source and Destination” in the “Usage Guidelines” section.
protocol	(Optional) Protocol number that the rule matches. Valid protocol numbers are 0x0 to 0xffff. For listings of valid protocol names, see “MAC Protocols” in the “Usage Guidelines” section.
cos *cos-value*	(Optional) Specifies that the rule matches only packets with an IEEE 802.1Q header that contains the Class of Service (CoS) value given in the *cos-value* argument. The *cos-value* argument can be an integer from 0 to 7.

vlan *VLAN-ID*	(Optional) Specifies that the rule matches only packets with an IEEE 802.1Q header that contains the VLAN ID given. The *VLAN-ID* argument can be an integer from 1 to 4094.
time-range *time-range-name*	(Optional) Specifies the time range that applies to this rule. You can configure a time range by using the **time-range** command.

Command Default

A newly created MAC ACL contains no rules.

If you do not specify a sequence number, the device assigns the rule a sequence number that is 10 greater than the last rule in the ACL.

Command Modes

MAC ACL configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

When the device applies a MAC ACL to a packet, it evaluates the packet with every rule in the ACL. The device enforces the first rule that has conditions that are satisfied by the packet. When the conditions of more than one rule are satisfied, the device enforces the rule with the lowest sequence number.

This command does not require a license.

Source and Destination

You can specify the *source* and *destination* arguments in one of two ways. In each rule, the method that you use to specify one of these arguments does not affect how you specify the other argument. When you configure a rule, use the following methods to specify the *source* and *destination* arguments:

- Address and mask—You can use a MAC address followed by a mask to specify a single address or a group of addresses. The syntax is as follows:

```
MAC-address MAC-mask
```

The following example specifies the *source* argument with the MAC address 00c0.4f03.0a72:

```
switch(config-acl)# deny 00c0.4f03.0a72 0000.0000.0000 any
```

The following example specifies the *destination* argument with a MAC address for all hosts with a MAC vendor code of 00603e:

```
switch(config-acl)# deny any 0060.3e00.0000 0000.0000.0000
```

- Any address—You can use the **any** keyword to specify that a source or destination is any MAC address. For examples of the use of the **any** keyword, see the examples in this section. Each of the examples shows how to specify a source or destination by using the **any** keyword.

MAC Protocols

The *protocol* argument can be the MAC protocol number or a keyword. The protocol number is a four-byte hexadecimal number prefixed with 0x. Valid protocol numbers are from 0x0 to 0xffff. Valid keywords are the following:

- **aarp—**Appletalk ARP (0x80f3)
- **appletalk—**Appletalk (0x809b)
- **decnet-iv—**DECnet Phase IV (0x6003)
- **diagnostic—**DEC Diagnostic Protocol (0x6005)
- **etype-6000—**EtherType 0x6000 (0x6000)
- **etype-8042—**EtherType 0x8042 (0x8042)
- **ip—**Internet Protocol v4 (0x0800)
- **lat—**DEC LAT (0x6004)
- **lavc-sca—**DEC LAVC, SCA (0x6007)
- **mop-console—**DEC MOP Remote console (0x6002)
- **mop-dump—**DEC MOP dump (0x6001)
- **vines-echo—**VINES Echo (0x0baf)

Examples

This example shows how to configure a MAC ACL named mac-ip-filter with rules that permit any non-IPv4 traffic between two groups of MAC addresses:

```
switch# configure terminal
switch(config)# mac access-list mac-ip-filter
switch(config-mac-acl)# deny 00c0.4f00.0000 0000.00ff.ffff 0060.3e00.0000 0000.00ff.ffff
ip
switch(config-mac-acl)# permit any any
```

Related Commands

Command	Description
mac access-list	Configures a MAC ACL.
permit (MAC)	Configures a deny rule in a MAC ACL.
remark	Configures a remark in an ACL.
show mac access-list	Displays all MAC ACLs or one MAC ACL.
statistics per-entry	Enables collection of statistics for each entry in an ACL.
time-range	Configures a time range.

deny (role-based access control list)

To configure a deny action in the security group access control list (SGACL), use the **deny** command. To remove the action, use the **no** form of this command.

[1]**deny** {**all**| **icmp**| **igmp**| **ip**}{**tcp**| **udp**} [{**src**| **dst**}{ | {**eq** | **gt**| **lt**| **neq**}| *port -number*}| **range** {*port-number 1*| *port-number 2*}[**log**]

no deny {**all**| **icmp**| **igmp**| **ip**}{**tcp**| **udp**} [{**src**| **dst**}{ | {**eq** | **gt**| **lt**| **neq**}| *port -number*}| **range** {*port-number 1*| *port-number 2*}[**log**]

Syntax Description

all	Specifies all traffic.
icmp	Specifies Internet Control Message Protocol (ICMP) traffic.
igmp	Specifies Internet Group Management Protocol (IGMP) traffic.
ip	Specifies IP traffic.
tcp	Specifies TCP traffic.
udp	Specifies User Datagram Protocol (UDP) traffic.
src	Specifies the source port number.
dst	Specifies the destination port number.
eq	Specifies equal to the port number.
gt	Specifies greater than the port number.
lt	Specifies less than the port number.
neq	Specifies not equal to the port number.
port-number	Port number for TCP or UDP. The range is from 0 to 65535.
range	Specifies a port range for TCP or UDP.
port-number1	First port in the range. The range is from 0 to 65535.
port-number2	Last port in the range. The range is from 0 to 65535.

1

log	(Optional) Specifies that packets matching this configuration be logged.

Command Default

None

Command Modes

role-based access control list

Command History

Release	Modification
5.0(2)	The **log** keyword was added to support the enabling of role-based access control list (RBACL) logging.
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

To enable RBACL logging, you must enable RBACL policy enforcement on the VLAN and VRF.

To enable RBACL logging, you must set the logging level of ACLLOG syslogs to 6 and the logging level of CTS manager syslogs to 5.

This command requires the Advanced Services license.

Examples

This example shows how to add a deny action to an SGACL and enable RBACL logging:

```
switch# configure terminal
switch(config)# cts role-based access-list MySGACL
switch(config-rbacl)# deny icmp log
```

This example shows how to remove a deny action from an SGACL:

```
switch# configure terminal
switch(config)# cts role-based access-list MySGACL
switch(config-rbacl)# no deny icmp log
```

Related Commands

Command	Description
cts role-based access-list	Configures Cisco TrustSec SGACLs.
feature cts	Enables the Cisco TrustSec feature.
show cts role-based access-list	Displays the Cisco TrustSec SGACL configuration.

description (identity policy)

To configure a description for an identity policy, use the **description** command. To revert to the default, use the **no** form of this command.

description *text*

no description

Syntax Description

"*text*"	Text string that describes the identity policy. The string is alphanumeric. The maximum length is 100 characters.

Command Default

None

Command Modes

Identity policy configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure the description for an identity policy:

```
switch# configure terminal
switch(config)# identity policy AdminPolicy
switch(config-id-policy)# description "Administrator identity policy"
```

This example shows how to remove the description from an identity policy:

```
switch# configure terminal
switch(config)# identity policy AdminPolicy
switch(config-id-policy)# no description
```

Related Commands

Command	Description
identity policy	Creates or specifies an identity policy and enters identity policy configuration mode.
show identity policy	Displays identity policy information.

description (user role)

To configure a description for a user role, use the **description** command. To revert to the default, use the **no** form of this command.

description *text*

no description

Syntax Description

text	Text string that describes the user role. The string is alphanumeric. The maximum length is 128 characters.

Command Default

None

Command Modes

User role configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You can include blank spaces in the user role description text.

This command does not require a license.

Examples

This example shows how to configure the description for a user role:

```
switch# configure terminal
switch(config)# role name MyRole
switch(config-role)# description User role for my user account.
```

This example shows how to remove the description from a user role:

```
switch# configure terminal
switch(config)# role name MyRole
switch(config-role)# no description
```

Related Commands

Command	Description
role name	Creates or specifies a user role and enters user role configuration mode.
show role	Displays user role information.

destination interface

To configure a destination for ACL capture packets, use the destination interface command.

destination interface ethernet *slot/port*

Syntax Description

ethernet	Specifies Ethernet IEEE 802.3z.
slot/port	Slot and port identifiers for the interface. The range is from 1 to 253.

Command Default

None

Command Modes

ACL capture configuration mode (config-acl-capture)

Command History

Release	Modification
5.2(1)	This command was introduced.

Usage Guidelines

Only the physical interface can be used for the destination. Port-channel interfaces and supervisor in-band ports are not supported.

Port channels and supervisor in-band ports are not supported as a destination for ACL capture.

ACL capture session destination interfaces do not support ingress forwarding and ingress MAC learning. If a destination interface is configured with these options, the monitor keeps the ACL capture session down. Use the show monitor session all command to see if ingress forwarding and MAC learning are enabled.

Note You can use the no switchport monitor command to disable ingress forwarding and MAC learning on the interface.

The source port of the packet and the ACL capture destination port cannot be part of the same ASIC. If both ports belong to the same ASIC, a message appears when you configure the destination ports for ACL capture, and the packet is not captured.

You can enter the destination interface command multiple times to add multiple destinations.

This command does not require a license.

Examples

This example shows how to configure a destination for ACL capture packets:

```
switch# configure terminal
```

```
switch(config)# monitor session 7 type acl-capture
switch(config-acl-capture)# destination interface ethernet 5/5
```

Related Commands

Command	Description
monitor session session type acl-capture	Configures an ACL capture session.

device

To add a supplicant device to the Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) identity profile exception list, use the **device** command. To remove a supplicant device, use the **no** form of this command.

device {**authenticate**| **not-authenticate**} {**ip-address** *ipv4-address* [*subnet-mask*]| **mac-address** *mac-address* [*mac-address-mask*]} **policy** *policy-name*

no device {**authenticate**| **not-authenticate**} {**ip-address** *ipv4-address* [*subnet-mask*]| **mac-address** *mac-address* [*mac-address-mask*]} **policy** *policy-name*

Syntax Description

authenticate	Specifies to allow authentication of the device using the policy.
not-authenticate	Specifies to not allow authentication of the device using the policy.
ip-address *ipv4-address*	Specifies the IPv4 address for the supplicant device in the A.B.C.D format.
subnet-mask	(Optional) IPv4 subnet mask for the IPv4 address.
mac-address *mac-address*	Specifies the MAC address for the supplicant device in the XXXX.XXXX.XXXX format.
mac-address-mask	(Optional) Mask for the MAC address.
policy *policy-name*	Specifies the policy to use for the supplicant device.

Command Default

None

Command Modes

Identity policy configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to add a device to the EAPoUDP identity profile:

```
switch# configure terminal
switch(config)# identity profile eapoupd
switch(config-id-policy)# device authenticate 10.10.1.1 255.255.255.245 policy AdminPolicy
```

This example shows how to remove a device from the EAPoUDP identity profile:

```
switch# configure terminal
switch(config)# identity profile eapoupd
switch(config-id-policy)# no device authenticate 10.10.2.2 255.255.255.245 policy UserPolicy
```

Related Commands

Command	Description
identity policy	Creates or specifies an identity policy and enters identity policy configuration mode.
show identity policy	Displays identity policy information.

device-role

To specify the role of the device attached to the port, use the **device-role** command in IPv6 snooping policy configuration mode or router advertisement (RA) guard policy configuration mode.

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

Syntax Description

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

Command Default

The device role is host.

Command Modes

RA guard policy configuration (config-ra-guard)

Command History

Release	Modification
8.0(1)	This command was introduced.

Usage Guidelines

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

Examples

The following example defines an RA guard policy name as raguard1, places the device in RA guard policy configuration mode, and configures the device as the host:

```
switch(config)# ipv6 nd raguard policy raguard1
switch(config-ra-guard)# device-role host
```

Related Commands

Command	Description
ipv6 nd raguard policy	Defines the RA guard policy name and enters RA guard policy configuration mode.

dot1x default

To reset the 802.1X global or interface configuration to the default, use the **dot1x default** command.

dot1x default

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must use the **feature dot1x** command before you configure 802.1X.

This command does not require a license.

Examples

This example shows how to set the global 802.1X parameters to the default:

```
switch# configure terminal
switch(config)# dot1x default
```

This example shows how to set the interface 802.1X parameters to the default:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# dot1x default
```

Related Commands

Command	Description
feature dot1x	Enables the 802.1X feature.
show dot1x	Displays 802.1X feature status information.

dot1x host-mode

To allow 802.1X authentication for either a single supplicant or multiple supplicants on an interface, use the **dot1x host-mode** command. To revert to the default, use the **no** form of this command.

dot1x host-mode {**multi-host**| **single-host**}

no dot1x host-mode

Syntax Description

mutli-host	Allows 802.1X authentication for multiple supplicants on the interface.
single-host	Allows 802.1X authentication for only a single supplicant on the interface.

Command Default

single-host

Command Modes

Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must use the **feature dot1x** command before you configure 802.1X.

This command does not require a license.

Examples

This example shows how to allow 802.1X authentication of multiple supplicants on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# dot1x host-mode multi-host
```

This example shows how to revert to the default host mode on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# no dot1x host-mode
```

Related Commands

Command	Description
feature dot1x	Enables the 802.1X feature.

Command	Description
show dot1x all	Displays all 802.1X information.

dot1x initialize

To initialize 802.1X authentication for supplicants, use the **dot1x initialize** command.

dot1x initialize [**interface ethernet** *slot* | *port*]

Syntax Description

interface ethernet *slot / port*	(Optional) Specifies the interface for 802.1X authentication initialization.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must use the **feature dot1x** command before you configure 802.1X.

This command does not require a license.

Examples

This example shows how to initialize 802.1X authentication for supplicants on the Cisco NX-OS device:

```
switch# dot1x initialize
```

This example shows how to initialize 802.1X authentication for supplicants on an interface:

```
switch# dot1x initialize interface ethernet 2/1
```

Related Commands

Command	Description
feature dot1x	Enables the 802.1X feature.
show dot1x all	Displays all 802.1X information.

dot1x mac-auth-bypass

To enable MAC address authentication bypass on interfaces with no 802.1X supplicants, use the **dot1x mac-auth-bypass** command. To disable MAC address authentication bypass, use the **no** form of this command.

dot1x mac-auth-bypass [eap]

no dot1x mac-auth-bypass

Syntax Description

eap	Specifies that the bypass use Extensible Authentication Protocol (EAP).

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must use the **feature dot1x** command before you configure 802.1X.

This command does not require a license.

Examples

This example shows how to enable MAC address authentication bypass:

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# dot1x mac-auth-bypass
```

This example shows how to disable MAC address authentication bypass:

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# no dot1x mac-auth-bypass
```

Related Commands

Command	Description
feature dot1x	Enables the 802.1X feature.
show dot1x all	Displays all 802.1X information.