K to P Commands

This chapter describes the Cisco NX-OS Security commands that begin with K to P.

key

To create a key or to enter the configuration mode for an existing key, use the **key** command. To remove the key, use the **no** form of this command.

key *key-ID*

no key *key-ID*

Syntax Description

key-ID	ID of the key to configure. This ID must be a whole number between 0 and 65535.

Defaults

None

Command Modes

Keychain configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

A new key contains no key strings.

This command does not require a license.

Examples

This example shows how to enter key configuration mode for key 13 in the glbp-keys keychain:

```
switch# configure terminal
switch(config)# key chain glbp-keys
switch(config-keychain)# key 13
switch(config-keychain-key)#
```

Related Commands

Command	Description
accept-lifetime	Configures an accept lifetime for a key.
key chain	Creates a keychain and enter keychain.
key-string	Configures the shared secret (text) for a specific key.
send-lifetime	Configures a send lifetime for a key.
show key chain	Shows keychain configuration.

key config-key

To configure the master key for type-6 encryption, use the **key config-key command. To delete the master key** and stop type-6 encryption**, use the no form of this command.**

key config-key ascii *new-master-key*

no key config-key ascii

Syntax Description

ascii	Specifies the ASCII format.
new-master-key	The master key. The master key can be a minimum of 16 to a maximum of 32 alphanumeric characters.

Defaults

None

Command Modes

Any command mode

Command History

Release	Modification
5.2(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure the master key for type-6 encryption:

```
switch# key config-key ascii
New Master Key:
Retype Master Key:

This example shows how to delete the master key and stop type-6 encryption:

switch# no key config-key ascii
Warning deletion of master-key will stop further type-6 encryption.
Do you want to proceed (y/n)[n]: [n] y

switch#
```

Related Commands

Command	Description
feature password encryption aes	Enables the AES password encryption features.
show encryption service stat	Displays the status of the encryption service.

key-string

To configure the text for a key, use the **key-string** command. To remove the text, use the **no** form of this command.

key-string [*encryption-type*] *text-string*

no key-string *text-string*

Syntax Description

encryption-type	(Optional) Type of encryption to use. The *encryption-type* argument can be one of the following values: • 0—The text-string argument that you enter is unencrypted text. This is the default. • 7—The text-string argument that you enter is encrypted. The encryption method is a Cisco proprietary method. This option is useful when you are entering a text string based on the encrypted output of a **show key chain** command that you ran on another Cisco NX-OS device.
text-string	Text of the key string, up to 63 case-sensitive, alphanumeric characters.

Defaults

None

Command Modes

Key configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The key-string text is a shared secret. The device stores key strings in a secure format.

You can obtain encrypted key strings by using the **show key chain** command on another Cisco NX-OS device.

This command does not require a license.

Examples

This example shows how to enter an encrypted shared secret for key 13:

```
switch# configure terminal
switch(config)# key chain glbp-keys
switch(config-keychain)# key 13
switch(config-keychain-key)# key-string 7 071a33595c1d0c1702170203163e3e21213c20361a021f11
switch(config-keychain-key)#
```

Related Commands

Command	Description
accept-lifetime	Configures an accept lifetime for a key.
key	Configures a key.
key chain	Configures a keychain.
send-lifetime	Configures a send lifetime for a key.
show key chain	Shows keychain configuration.

key chain

To create a keychain or to configure an existing keychain, use the **key chain** command. To remove the keychain, use the **no** form of this command.

key chain *keychain-name*

no key chain *keychain-name*

Syntax Description

keychain-name	Name of the keychain, up to 63 alphanumeric, case-sensitive characters in length.

Defaults

None

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command creates the keychain if it does not already exist. A new keychain contains no keys.

Removing a keychain also removes any keys that the keychain contains.

Before you remove a keychain, ensure that no feature uses it. If a feature is configured to use a keychain that you remove, that feature is likely to fail to communicate with other devices.

This command does not require a license.

Examples

This example shows how to configure a keychain named glbp-keys:

```
switch# configure terminal
switch(config)# key chain glbp-keys
switch(config-keychain)#
```

Related Commands

Command	Description
accept-lifetime	Configures an accept lifetime for a key.
key	Configures a key.
key-string	Configures a key string.
send-lifetime	Configures a send lifetime for a key.
show key chain	Configures a send lifetime for a key.

ldap-server deadtime

To configure the deadtime interval for all Lightweight Directory Access Protocol (LDAP) servers, use the **ldap-server deadtime** command. The deadtime interval specifies the time that the Cisco NX-OS device waits, after declaring that an LDAP server is dead, before sending out a test packet to determine if the server is now alive. To remove the global deadtime interval configuration, use the **no** form of this command.

ldap-server deadtime *minutes*

no ldap-server deadtime *minutes*

Syntax Description

minutes	Global deadtime interval for LDAP servers. The range is from 1 to 60 minutes.

Defaults

0 minutes

Command Modes

Global configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable LDAP.

When the dead-time interval is 0 minutes, LDAP servers are not marked as dead even if they are not responding.

This command does not require a license.

Examples

This example shows how to configure the global deadtime interval for LDAP servers:

```
switch# config t
switch(config)# ldap-server deadtime 5
```

Related Commands

Command	Description
feature ldap	Enables LDAP.
show ldap-server	Displays the LDAP server configuration.

ldap-server host

To configure Lightweight Directory Access Protocol (LDAP) server host parameters, use the **ldap-server host** command. To revert to the defaults, use the **no** form of this command.

ldap-server host {*ipv4-address* | *ipv6-address* | *host-name*}
[**enable-ssl**]
[**port** *tcp-port* [**timeout** *seconds*]]
[**rootDN** *root-name* [**password** *password*] [**port** *tcp-port* [**timeout** *seconds*] | [**timeout** *seconds*]]]
[**test rootDN** *root-name* [**idle-time** *minutes* | **password** *password* [**idle-time** *minutes*] | **username** *name* [**password** *password* [**idle-time** *minutes*]]]]
[**timeout** *seconds*]

no ldap-server host {*ipv4-address* | *ipv6-address* | *host-name*}
[**enable-ssl**]
[**port** *tcp-port* [**timeout** *seconds*]]
[**rootDN** *root-name* [**password** *password*] [**port** *tcp-port* [**timeout** *seconds*] | [**timeout** *seconds*]]]
[**test rootDN** *root-name* [**idle-time** *minutes* | **password** *password* [**idle-time** *minutes*] | **username** *name* [**password** *password* [**idle-time** *minutes*]]]]
[**timeout** *seconds*]

Syntax Description

ipv4-address	Server IPv4 address in the *A.B.C.D* format.
ipv6-address	Server IPv6 address in the *X:X:X:X* format.
host-name	Server name. The name is alphanumeric, case sensitive, and has a maximum of 256 characters.
enable-ssl	(Optional) Ensures the integrity and confidentiality of the transferred data by causing the LDAP client to establish a Secure Sockets Layer (SSL) session before sending the bind or search request.
port *tcp-port*	(Optional) Specifies the TCP port to use for LDAP messages to the server. The range is from 1 to 65535.
timeout *seconds*	(Optional) Specifies the timeout interval for the server. The range is from 1 to 60 seconds.
rootDN *root-name*	(Optional) Specifies the root designated name (DN) for the LDAP server database. You can enter up to 128 alphanumeric characters for the root name.
password *password*	(Optional) Specifies the bind password for the root.
test	(Optional) Configures parameters to send test packets to the LDAP server.
idle-time *minutes*	Specifies the time interval (in minutes) for monitoring the server. The range is from 1 to 1440 minutes.
username *name*	Specifies a username in the test packets. The username is alphanumeric, case sensitive, and has a maximum of 32 characters. **Note** To protect network security, we recommend that you use a username that is not the same as an existing username in the LDAP database.

Defaults

Server monitoring: Disabled
TCP port: The global value or 389 if a global value is not configured
Timeout: The global value or 5 seconds if a global value is not configured
Idle time: 60 minutes
Test username: test
Test password: Cisco

Command Modes

Global configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable LDAP and obtain the IPv4 or IPv6 address or hostname for the remote LDAP server.

If you plan to enable the SSL protocol, make sure that the LDAP server certificate is manually configured on the Cisco NX-OS device.

By default, when you configure an LDAP server IP address or hostname on the Cisco NX-OS device, the LDAP server is added to the default LDAP server group. You can also add the LDAP server to another LDAP server group.

The timeout interval value specified for an LDAP server overrides the global timeout interval value specified for all LDAP servers.

This command does not require a license.

Examples

This example shows how to configure the IPv6 address for an LDAP server:

```
switch# config t
switch(config)# ldap-server host 10.10.2.2 timeout 20
```

This example shows how to configure the parameters for LDAP server monitoring:

```
switch# config t
switch(config)# ldap-server host 10.10.1.1 test rootDN root1 username user1 password
Ur2Gd2BH idle-time 3
```

Related Commands

Command	Description
feature ldap	Enables LDAP.
show ldap-server	Displays the LDAP server configuration.

ldap-server port

To configure a global Lightweight Directory Access Protocol (LDAP) server port through which clients initiate TCP connections, use the **ldap-server port** command. To remove the LDAP server port configuration, use the **no** form of this command.

ldap-server port *tcp-port*

no ldap-server port *tcp-port*

Syntax Description

tcp-port	Global TCP port to use for LDAP messages to the server. The range is from 1 to 65535.

Defaults

TCP port 389

Command Modes

Global configuration

Command History

Release	Modification
5.2(1)	This command was deprecated.
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable LDAP.

This command does not require a license.

Examples

This example shows how to configure a global TCP port for LDAP messages:

```
switch# config t
switch(config)# ldap-server port 2
```

Related Commands

Command	Description
feature ldap	Enables LDAP.
show ldap-server	Displays the LDAP server configuration.

ldap-server timeout

To configure a global timeout interval that determines how long the Cisco NX-OS device waits for responses from all Lightweight Directory Access Protocol (LDAP) servers before declaring a timeout failure, use the **ldap-server timeout** command. To remove the global timeout configuration, use the **no** form of this command.

ldap-server timeout *seconds*

no ldap-server timeout *seconds*

Syntax Description

seconds	Timeout interval for LDAP servers. The range is from 1 to 60 seconds.

Defaults

5 seconds

Command Modes

Global configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable LDAP.

This command does not require a license.

Examples

This example shows how to configure the global timeout interval for LDAP servers:

```
switch# config t
switch(config)# ldap-server timeout 10
```

Related Commands

Command	Description
feature ldap	Enables LDAP.
show ldap-server	Displays the LDAP server configuration.

ldap search-map

To configure a Lightweight Directory Access Protocol (LDAP) search map to send a search query to the LDAP server, use the **ldap search-map** command. To disable the search map, use the **no** form of this command.

ldap search-map *map-name*

no ldap search-map *map-name*

Syntax Description

map-name	Name of the LDAP search map. The name is alphanumeric, case sensitive, and has a maximum of 128 characters.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable LDAP.

This command does not require a license.

Examples

This example shows how to configure an LDAP search map:

```
switch# config t
switch(config)# ldap search-map map1
```

Related Commands

Command	Description
feature ldap	Enables LDAP.
show ldap-search-map	Displays the configured LDAP search maps.
CRLLookup	Configures the attribute name, search filter, and base-DN for the CRL search operation in order to send a search query to the LDAP server.
trustedCert	Configures the attribute name, search filter, and base-DN for the trusted certificate search operation in order to send a search query to the LDAP server.
user-certdn-match	Configures the attribute name, search filter, and base-DN for the certificate DN match search operation in order to send a search query to the LDAP server.

Command	Description
user-pubkey-match	Configures the attribute name, search filter, and base-DN for the public key match search operation in order to send a search query to the LDAP server.
user-switch-bind	Configures the attribute name, search filter, and base-DN for the user-switchgroup search operation in order to send a search query to the LDAP server.
userprofile	Configures the attribute name, search filter, and base-DN for the user profile search operation in order to send a search query to the LDAP server.

logging drop threshold

To configure the threshold value for dropped packets and generate a syslog if the drop count exceeds the configured threshold in a policy map for Control Plane Policing (CoPP), use the **logging drop threshold** command.

logging drop threshold [*drop-count* [**level** *syslog-level*]]

Syntax Description

drop-count	Drop count. The range is from 1 to 80000000000.
level	(Optional) Specifies the syslog level.
syslog-level	Syslog level. The range is from 1 to 7.

Defaults

Syslog level 4

Command Modes

config-pmap-c

Command History

Release	Modification
5.1(1)	This command was introduced.

Usage Guidelines

Ensure that you are in the default VDC.

Ensure that you have configured the IP ACLs if you want to use ACE hit counters in the class maps.

This command does not require a license.

Examples

This example shows how to configure the threshold value for dropped packets and generate a syslog if the drop count exceeds the configured threshold in a policy map for CoPP:

```
switch# config t
switch(config)# policy-map type control-plane ClassMapA
switch(config-pmap)# class ClassMapA
switch(config-pmap-c)# police cir 52000
switch(config-pmap-c)# police cir 52000 bc 2000
switch(config-pmap-c)# police cir 5000 conform transmit exceed drop violate set1 dscp3
dscp4 table1 pir-markdown-map
switch(config-pmap-c)# police cir 52000 pir 78000 be 2000
switch(config-pmap-c)# logging drop threshold 1800 level 2
switch(config-pmap-c)#
```

Related Commands

Command	Description
policy-map type control-plane	Configures a control plane policy map and enters policy map configuration mode.

lt

To specify a less-than group member for an IP port object group, use the **lt** command. A less-than group member matches port numbers that are less than (and not equal to) the port number specified in the entry. To remove a greater-than group member from port object group, use the **no** form of this command.

[*sequence-number*] **lt** *port-number*

no {*sequence-number* | **lt** *port-number*}

Syntax Description

sequence-number	(Optional) Sequence number for this group member. Sequence numbers maintain the order of group members within an object group. Valid sequence numbers are from 1 to 4294967295. If you do not specify a sequence number, the device assigns a number that is 10 greater than the largest sequence number in the current object group.
port-number	Port number that traffic matching this group member does not exceed or equal. Valid values are from 0 to 65535.

Defaults

None

Command Modes

IP port object group configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

IP port object groups are not directional. Whether a **lt** command matches a source or destination port or whether it applies to inbound or outbound traffic depends upon how you use the object group in an ACL.

This command does not require a license.

Examples

This example shows how to configure an IP port object group named port-group-05 with a group member that matches traffic sent to or from port 1 through port 49151:

```
switch# config t
switch(config)# object-group ip port port-group-05
switch(config-port-ogroup)# lt 49152
```

Related Commands

Command	Description
eq	Specifies an equal-to group member in an IP port object group.
gt	Specifies a greater-than group member in an IP port object group.
neq	Specifies a not-equal-to group member in an IP port object group.

Command	Description
object-group ip port	Configures an IP port object group.
range	Specifies a port range group member in an IP port object group.
show object-group	Displays object groups.

mac access-list

To create a MAC access control list (ACL) or to enter MAC access list configuration mode for a specific ACL, use the **mac access-list** command. To remove a MAC ACL, use the **no** form of this command.

mac access-list *access-list-name*

no mac access-list *access-list-name*

Syntax Description

access-list-name	Name of the MAC ACL, which can be up to 64 alphanumeric, case-sensitive characters long but cannot contain a space or a quotation mark.

Defaults

None

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

No MAC ACLs are defined by default.

Use MAC ACLs to filter non-IP traffic. If you disable packet classification, you can use MAC ACLs to filter all traffic.

When you use the **mac access-list** command, the device enters MAC access list configuration mode, where you can use the MAC **deny** and **permit** commands to configure rules for the ACL. If the ACL specified does not exist, the device creates it when you enter this command.

Use the **mac port access-group** command to apply the ACL to an interface.

Every MAC ACL has the following implicit rule as its last rule:

```
deny any any protocol
```

This implicit rule ensures that the device denies the unmatched traffic, regardless of the protocol specified in the Layer 2 header of the traffic.

Use the **statistics per-entry** command to configure the device to record statistics for each rule in a MAC ACL. The device does not record statistics for implicit rules. To record statistics for packets that would match the implicit rule, you must explicitly configure a rule to deny the packets.

This command does not require a license.

Examples

This example shows how to enter MAC access list configuration mode for a MAC ACL named mac-acl-01:

```
switch# conf t
switch(config)# mac access-list mac-acl-01
switch(config-acl)#
```

Related Commands

Command	Description
deny (MAC)	Configures a deny rule in a MAC ACL.
mac port access-group	Applies a MAC ACL to an interface.
permit (MAC)	Configures a permit rule in a MAC ACL.
show mac access-lists	Displays all MAC ACLs or a specific MAC ACL.
statistics per-entry	Enables collection of statistics for each entry in an ACL.

mac packet-classify

To enable MAC packet classification on a Layer 2 interface, use the **mac packet-classify** command. To disable MAC packet classification, use the **no** form of this command.

mac packet-classify

no mac packet-classify

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Interface configuration

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

MAC packet classification allows you to control whether a MAC ACL that is on a Layer 2 interface applies to all traffic entering the interface, including IP traffic, or to non-IP traffic only.

When MAC packet classification is enabled on a Layer 2 interface, a MAC ACL that is on the interface applies to all traffic entering the interface, including IP traffic. Also, you cannot apply an IP port ACL on the interface.

When MAC packet classification is disabled on a Layer 2 interface, a MAC ACL that is on the interface applies only to non-IP traffic entering the interface. Also, you can apply an IP port ACL on the interface.

To configure an interface as a Layer 2 interface, use the **switchport** command.

Examples

This example shows how to configure an Ethernet interface to operate as a Layer 2 interface and to enable MAC packet classification:

```
switch# conf t
switch(config)# interface ethernet 2/3
switch(config-if)# switchport
switch(config-if)# mac packet-classify
switch(config-if)#
```

This example shows how to view the configuration of an Ethernet interface and the error message that appears if you try to apply an IP port ACL to the interface when MAC packet classification is enabled:

```
switch(config)# show running-config interface ethernet 2/3

!Command: show running-config interface Ethernet2/3
!Time: Wed Jun 24 13:06:49 2009
```

```
version 4.2(1)

interface Ethernet2/3
  ip access-group ipacl in
  mac port access-group macacl
  switchport
  mac packet-classify

switch(config)# interface ethernet 2/3
switch(config-if)# ip port access-group ipacl in
ERROR: The given policy cannot be applied as mac packet classification is enable
d on this port
switch(config-if)#
```

Related Commands

Command	Description
ip port access-group	Applies a IPv4 ACL to an interface as a port ACL.
ipv6 port traffic-filter	Applies a IPv6 ACL to an interface as a port ACL.
switchport	Configures an interface to operate as a Layer 2 interface.

mac port access-group

To apply a MAC access control list (ACL) to an interface, use the **mac port access-group** command. To remove a MAC ACL from an interface, use the **no** form of this command.

mac port access-group *access-list-name*

no mac port access-group *access-list-name*

Syntax Description

access-list-name	Name of the MAC ACL, which can be up to 64 alphanumeric, case-sensitive characters.

Defaults

None

Command Modes

Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

By default, no MAC ACLs are applied to an interface.

MAC ACLs apply to non-IP traffic, unless the device is configured to not classify traffic based on Layer 3 headers. If packet classification is disabled, MAC ACLs apply to all traffic.

You can use the **mac port access-group** command to apply a MAC ACL as a port ACL to the following interface types:

- Layer 2 interfaces
- Layer 2 Ethernet port-channel interfaces

You can also apply a MAC ACL as a VLAN ACL. For more information, see the **match (VLAN access-map)** command.

The device applies MAC ACLs only to inbound traffic. When the device applies a MAC ACL, the device checks packets against the rules in the ACL. If the first matching rule permits the packet, the device continues to process the packet. If the first matching rule denies the packet, the device drops the packet and returns an ICMP host-unreachable message.

If you delete the specified ACL from the device without removing the ACL from an interface, the deleted ACL does not affect traffic on the interface.

This command does not require a license.

Examples

This example shows how to apply a MAC ACL named mac-acl-01 to Ethernet interface 2/1:

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# mac port access-group mac-acl-01
```

This example shows how to remove a MAC ACL named mac-acl-01 from Ethernet interface 2/1:

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# no mac port access-group mac-acl-01 in
```

Related Commands

Command	Description
mac access-list	Configures a MAC ACL.
show access-lists	Displays all ACLs.
show mac access-lists	Shows either a specific MAC ACL or all MAC ACLs.
show running-config interface	Shows the running configuration of all interfaces or of a specific interface.

match (class-map)

To configure match criteria for control place class maps, use the **match** command. To delete match criteria for a control plane policy map, use the **no** form of the command.

match access-group name *access-list*

match exception {[**ip** [**unicast rpf-failure**] | **ipv6**] {**icmp** {**redirect** | **unreachable**} | **option**}}

match protocol arp

match redirect {**arp-inspect** | **dhcp-snoop**}

no match access-group name *access-list*

no match exception {[**ip** [**unicast rpf-failure**] | **ipv6**] {**icmp** {**redirect** | **unreachable**} | **option**}}

no match protocol arp

no match redirect {**arp-inspect** | **dhcp-snoop**}

Syntax Description

access-group name *access-list*	Matches an IP or MAC access control list.
exception	Matches exception packets.
ip	(Optional) Matches IPv4 exception packets.
ipv6	(Optional) Matches IPv6 exception packets.
unicast rpf-failure	(Optional) Matches IPv4 Unicast Reverse Path Forwarding (Unicast RPF) packets.
icmp	Matches IPv4 or IPv6 ICMP packets.
redirect	Matches IPv4 or IPv6 ICMP redirect packets.
unreachable	Matches IPv4 or IPv6 ICMP unreachable packets.
option	Matches IPv4 or IPv6 option packets.
protocol arp	Matches Address Resolution Protocol (ARP) packets.
redirect	Matches dynamic ARP inspection or DHCP snooping redirect packets.
arp-inspect	Matches dynamic ARP inspection.
dhcp-snoop	Matches dynamic DHCP snooping.

Defaults

None

Command Modes

Class map configuration

Command History

Release	Modification
6.2(10)	The **unicast rpf-failure** keywords were added.

4.0(3)	Added support for policing IPv6 packets.
4.0(1)	This command was introduced.

Usage Guidelines

You must create the IP ACLs or MAC ACLs before you reference them in this command.

You can use this command only in the default VDC.

This command does not require a license.

Examples

This example shows how to specify a match criteria for a control plane class map:

```
switch# config t
switch(config)# class-map type control-plane ClassMapA
switch(config-pmap)# match exception ip icmp redirect
switch(config-pmap)# match redirect arp-inspect
```

This example shows how to remove a criteria for a control plane class map:

```
switch# config t
switch(config)# class-map type control-plane ClassMapA
switch(config-pmap)# no match exception ip icmp redirect
```

Related Commands

Command	Description
class-map type control-plane	Creates or specifies a control plane class map and enters class map configuration mode.
show class-map type control-plane	Displays configuration information for control plane policy maps.

match (VLAN access-map)

To specify an access control list (ACL) for traffic filtering in a VLAN access map, use the **match** command. To remove a **match** command from a VLAN access map, use the **no** form of this command.

match {**ip** | **ipv6** | **mac**} **address** *access-list-name*

no match {**ip** | **ipv6** | **mac**} **address** *access-list-name*

Syntax Description

ip	Specifies that the ACL is an IPv4 ACL.
ipv6	Specifies that the ACL is an IPv6 ACL.
mac	Specifies that the ACL is a MAC ACL.
address *access-list-name*	Specifies the ACL by name, which can be up to 64 alphanumeric, case-sensitive characters.

Defaults

None

Command Modes

VLAN access-map configuration

Command History

Release	Modification
4.1(2)	The **ipv6** keyword was added.
4.0(1)	This command was introduced.

Usage Guidelines

You can specify one or more **match** commands per entry in a VLAN access map.

By default, the device classifies traffic and applies IPv4 ACLs to IPv4 traffic, IPv6 ACLs to IPv6 traffic, and MAC ACLs to all other traffic.

This command does not require a license.

Examples

This example shows how to create a VLAN access map named vlan-map-01 and add two entries that each have two **match** commands and one **action** command:

```
switch(config-access-map)# vlan access-map vlan-map-01
switch(config-access-map)# match ip address ip-acl-01
switch(config-access-map)# action forward
switch(config-access-map)# match mac address mac-acl-00f
switch(config-access-map)# vlan access-map vlan-map-01
switch(config-access-map)# match ip address ip-acl-320
switch(config-access-map)# match mac address mac-acl-00e
switch(config-access-map)# action drop
switch(config-access-map)# show vlan access-map

Vlan access-map vlan-map-01 10
        match ip: ip-acl-01
```

```
        match mac: mac-acl-00f
        action: forward
Vlan access-map vlan-map-01 20
        match ip: ip-acl-320
        match mac: mac-acl-00e
        action: drop
```

Related Commands

Command	Description
action	Specifies an action for traffic filtering in a VLAN access map.
show vlan access-map	Displays all VLAN access maps or a VLAN access map.
show vlan filter	Displays information about how a VLAN access map is applied.
vlan access-map	Configures a VLAN access map.
vlan filter	Applies a VLAN access map to one or more VLANs.

monitor session

To configure an access control list (ACL) capture session in order to selectively monitor traffic on an interface or VLAN, use the **monitor session** command.

monitor session *session* **type acl-capture**

Syntax Description

session	Session ID. The range is from 0 to 48.
type	Specifies a session type.
acl-capture	Creates an ACL capture session.

Defaults

None

Command Modes

Global configuration

Command History

Release	Modification
5.2(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure an ACL capture session:

```
switch# configure terminal
switch(config)# monitor session 5 type acl-capture
switch(config-acl-capture)#
```

Related Commands

Command	Description
access-list capture	Enables access control list (ACL) capture on all virtual device contexts (VDCs).
destination interface	Configures a destination for ACL capture packets.
show ip-access capture session	Displays the ACL capture session configuration.

nac enable

To enable Network Admission Control (NAC) on an interface, use the **nac enable** command. To disable NAC, use the **no** form of this command.

nac enable

no nac enable

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must use the **feature eou** command and set the switchport mode to access before using the **nac enable** command.

You can enable EAPoUDP only on an access mode interface.

This command does not require a license.

Examples

This example shows how to enable NAC on an interface:

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# switchport
switch(config-if)# switchport mode access
switch(config-if)# nac enable
```

This example shows how to disable NAC on an interface:

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# no nac enable
```

Related Commands

Command	Description
feature eou	Enables EAPoUDP.
show eou	Displays EAPoUDP information.

neq

To specify a not-equal-to group member for an IP port object group, use the **neq** command. To remove a not-equal-to group member from port object group, use the **no** form of this command.

[*sequence-number*] **neq** *port-number*

no {*sequence-number* | **neq** *port-number*}

Syntax Description

sequence-number	(Optional) Sequence number for this group member. Sequence numbers maintain the order of group members within an object group. Valid sequence numbers are from 1 to 4294967295. If you do not specify a sequence number, the device assigns a number that is 10 greater than the largest sequence number in the current object group.
port-number	Port number that this group member does not match. Valid values are from 0 to 65535.

Defaults

None

Command Modes

IP port object group configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

A not-equal-to group member matches port numbers that are not equal to the port number specified in the entry.

IP port object groups are not directional. Whether an **neq** command matches a source or destination port or whether it applies to inbound or outbound traffic depends upon how you use the object group in an ACL.

This command does not require a license.

Examples

This example shows how to configure an IP port object group named port-group-05 with a group member that matches traffic sent to any port except port 80:

```
switch# config t
switch(config)# object-group ip port port-group-05
switch(config-port-ogroup)# neq 80
```

Related Commands

Command	Description
eq	Specifies an equal-to group member in an IP port object group.
gt	Specifies a greater-than group member in an IP port object group.
lt	Specifies a less-than group member in an IP port object group.
object-group ip port	Configures an IP port object group.
range	Specifies a port-range group member in an IP port object group.
show object-group	Displays object groups.

object-group (identity policy)

To specify a MAC access control list (ACL) for an identity policy, use the **object-group** command. To remove ACL from the identity policy, use the **no** form of this command.

object-group *acl-name*

no object-group *acl-name*

Syntax Description

acl-name	Name of a MAC ACL. The name is case sensitive.

Defaults

None

Command Modes

Identity policy configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **mac access-list** command to create the MAC ACL to assign to the identity policy.

This command does not require a license.

Examples

This example shows how to configure an ACL for an identity policy:

```
switch# config t
switch(config)# identity policy AdminPolicy
switch(config-id-policy)# object-group
```

This example shows how to remove an ACL from an identity policy:

```
switch# config t
switch(config)# identity policy AdminPolicy
switch(config-id-policy)# no object-group
```

Related Commands

Command	Description
identity policy	Creates or specifies an identity policy and enters identity policy configuration mode.
mac access-list	Creates a MAC ACL and enters MAC ACL configuration mode.
show identity policy	Displays identity policy information.

object-group ip address

To define an IPv4 address object group or to enter object-group configuration mode for a specific IPv4-address object group, use the **object-group ip address** command. To remove an IPv4-address object group, use the **no** form of this command.

object-group ip address *name*

no object-group ip address *name*

Syntax Description

name	Name of the IPv4 address object group, which can be up to 64 alphanumeric, case-sensitive characters.

Defaults

None

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You can use IPv4 object groups in **permit** and **deny** commands for IPv4 access control lists (ACLs).

IPv4 address object groups are not directional. Whether group members match a source or destination address or whether an object group applies to inbound or outbound traffic depends upon how you use the object group in an IPv4 ACL.

This command does not require a license.

Examples

This example shows how to configure an IPv4 address object group named ipv4-addr-group-13 with two group members that are specific IPv4 addresses and one group member that is the 10.23.176.0 subnet:

```
switch# config t
switch(config)# object-group ip address ipv4-addr-group-13
switch(config-ipaddr-ogroup)# host 10.121.57.102
switch(config-ipaddr-ogroup)# 10.121.57.234/32
switch(config-ipaddr-ogroup)# 10.23.176.0 0.0.0.255
switch(config-ipaddr-ogroup)# show object-group ipv4-addr-group-13
        10 host 10.121.57.102
        20 host 10.121.57.234
        30 10.23.176.0/24
switch(config-ipaddr-ogroup)#
```

Related Commands

Command	Description
host (IPv4)	Configures a group member for an IPv4 address object group.
show object-group	Displays object groups.

object-group ip port

To define an IP port object group or to enter object-group configuration mode for a specific IP port object group, use the **object-group ip port** command. To remove an IP port object group, use the **no** form of this command.

object-group ip port *name*

no object-group ip port *name*

Syntax Description

name	Name of the IP port object group, which can be up to 64 alphanumeric, case-sensitive characters.

Defaults

None

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You can use IP port object groups in **permit** and **deny** commands for IPv4 and IPv6 access control lists (ACLs).

IP port object groups are not directional. Whether group members match a source or destination port or whether an object group applies to inbound or outbound traffic depends upon how you use the object group in an ACL.

This command does not require a license.

Examples

This example shows how to configure an IP port object group named port-group-05 with a group member that matches traffic sent to or from port 443:

```
switch# config t
switch(config)# object-group ip port port-group-05
switch(config-port-ogroup)# eq 443
switch(config-port-ogroup)# show object-group port-group-05
        10 eq 443
switch(config-port-ogroup)#
```

Related Commands

Command	Description
eq	Specifies an equal-to group member in an IP port object group.
gt	Specifies a greater-than group member in an IP port object group.

Command	Description
lt	Specifies a less-than group member in an IP port object group.
neq	Specifies a not-equal-to group member in an IP port object group.
range	Specifies a port range group member in an IP port object group.
show object-group	Displays object groups.

object-group ipv6 address

To define an IPv6 address object group or to enter IPv6 address object group configuration mode for a specific IPv6 address object group, use the **object-group ipv6 address** command. To remove an IPv6 address object group, use the **no** form of this command.

object-group ipv6 address *name*

no object-group ipv6 address *name*

Syntax Description

name	Name of the IPv6 address group object, which can be up to 64 alphanumeric, case-sensitive characters.

Defaults

None

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You can use IPv6 object groups in **permit** and **deny** commands for IPv6 ACLs.

IPv6 address object groups are not directional. Whether group members match a source or destination address or whether an object group applies to inbound or outbound traffic depends upon how you use the object group in an IPv6 ACL.

This command does not require a license.

Examples

This example shows how to configure an IPv6 address object group named ipv6-addr-group-A7 with two group members that are specific IPv6 addresses and one group member that is the 2001:db8:0:3ab7:: subnet:

```
switch# config t
switch(config)# object-group ipv6 address ipv6-addr-group-A7
switch(config-ipv6addr-ogroup)# host 2001:db8:0:3ab0::1
switch(config-ipv6addr-ogroup)# 2001:db8:0:3ab0::2/128
switch(config-ipv6addr-ogroup)# 2001:db8:0:3ab7::/96
switch(config-ipv6addr-ogroup)# show object-group ipv6-addr-group-A7
        10 host 2001:db8:0:3ab0::1
        20 host 2001:db8:0:3ab0::2
        30 2001:db8:0:3ab7::/96
switch(config-ipv6addr-ogroup)#
```

Related Commands

Command	Description
host (IPv6)	Configures a group member for an IPv6 address object group.
show object-group	Displays object groups.

object-group udp relay ip address

To configure an object group that consists of destination IP addresses to which the packets are forwarded, use the **object-group udp relay ip address** command.

object-group udp relay ip address *object-grp-name*

no object-group udp relay ip address *object-grp-name*

Syntax Description

object-grp-name	Specifies the name of the object group.

Defaults

None

Command Modes

Global configuration

Command History

Release	Modification
7.3(0)D1(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the UDP relay feature by using the **ip forward-protocol udp** command. You can create up to 4096 object groups.

Examples

This example shows how to configure the object group:

```
switch# configure terminal
switch(config)# ip forward-protocol udp
switch(config)# object-group udp relay ip address udprelay1
```

This example shows how to delete the the object group:

```
switch(config)# no object-group udp relay ip address udprelay1
```

Related Commands

Command	Description
ip forward-protocol udp	Enables the UDP relay feature.

password secure-mode

To enable secure mode for password changing, use the **password secure-mode** command. To disable the secure mode for password changing, use the **no** form of this command.

password secure-mode

no password secure-mode

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Global configuration

Command History

Release	Modification
6.1.4	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to enable secure mode for changing password:

```
switch# configure terminal
switch(config)# password secure-mode
```

This example shows how to disable secure mode for changing password:

```
switch# configure terminal
switch(config)# no password secure-mode
```

Related Commands

Command	Description
show password strength-check	Enables password-strength checking.

password strength-check

To enable password-strength checking, use the **password strength-check** command. To disable password-strength checking, use the **no** form of this command.

password strength-check

no password strength-check

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
4.0(3)	This command was introduced.

Usage Guidelines

When you enable password-strength checking, the Cisco NX-OS software only allows you to create strong passwords. The characteristics for strong passwords include the following:

- At least eight characters long
- Does not contain many consecutive characters (such as “abcd”)
- Does not contain many repeating characters (such as “aaabbb”)
- Does not contain dictionary words
- Does not contain proper names
- Contains both uppercase and lowercase characters
- Contains numbers

The following are examples of strong passwords:

- If2CoM18
- 2004AsdfLkj30
- Cb1955S21

Note When you enable password-strength checking, the Cisco NX-OS software does not check the strength of existing passwords.

This command does not require a license.

Examples

This example shows how to enable password-strength checking:

```
switch# configure terminal
switch(config)# password strength-check
```

This example shows how to disable password-strength checking:

```
switch# configure terminal
switch(config)# no password strength-check
```

Related Commands

Command	Description
show password strength-check	Enables password-strength checking.
show running-config security	Displays security feature configuration in the running configuration.

periodic

To specify a time range that is active one or more times per week, use the **periodic** command. To remove a periodic time range, use the **no** form of this command.

[*sequence-number*] **periodic** *weekday time* **to** [*weekday*] *time*

no {*sequence-number* | **periodic** *weekday time* **to** [*weekday*] *time*}

[*sequence-number*] **periodic** *list-of-weekdays time* **to** *time*

no {*sequence-number* | **periodic** *list-of-weekdays time* **to** *time*}

Syntax Description

sequence-number	(Optional) Sequence number of the rule, which causes the device to insert the command in that numbered position in the time range. Sequence numbers maintain the order of rules within a time range. A sequence number can be any integer between 1 and 4294967295. By default, the first rule in a time range has a sequence number of 10. If you do not specify a sequence number, the device adds the rule to the end of the time range 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.
weekday	Day of the week that the range begins or ends. The first occurrence of this argument is the day that the range starts. The second occurrence is the day that the range ends. If the second occurrence is omitted, the end of the range is on the same day as the start of the range. The following keywords are valid values for the *weekday* argument: • **monday** • **tuesday** • **wednesday** • **thursday** • **friday** • **saturday** • **sunday**
time	Time of day that the range starts or ends. The first occurrence of this argument is the time that the range begins. The second occurrence of this argument is the time that the range ends. You can specify the *time* argument in 24-hour notation, in the format *hours*:*minutes* or *hours*:*minutes*:*seconds*. For example, 8:00 a.m. is 8:00 and 8:00 p.m. is 20:00.
to	Separates the first and second occurrences of the *time* argument.

list-of-weekdays	(Optional) Days that the range is in effect. Valid values of this argument are as follows: • A space-delimited list of weekdays, such as the following: **monday thursday friday** • **daily**—All days of the week. • **weekdays**—Monday through Friday. • **weekend**—Saturday through Sunday.

Defaults

to

Command Modes

Time-range 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 create a time range named weekend-remote-access-times and configure a periodic rule that allows traffic between 4:00 a.m. and 10:00 p.m. on Saturday and Sunday:

```
switch# config t
switch(config)# time-range weekend-remote-access-times
switch(config-time-range)# periodic weekend 04:00:00 to 22:00:00
```

This example shows how to create a time range named mwf-evening and configure a periodic rule that allows traffic between 6:00 p.m. and 10:00 p.m. on Monday, Wednesday, and Friday:

```
switch# config t
switch(config)# time-range mwf-evening
switch(config-time-range)# periodic monday wednesday friday 18:00:00 to 22:00:00
```

Related Commands

Command	Description
absolute	Configures an absolute time-range rule.
time-range	Configures a time range that you can use in IPv4 and IPv6 ACLs.

permit (ACL)

To enable a capture session for the access control entries (ACEs) of the access control list, use the **permit** command.

permit protocol {**0-255** | **ahp** | **eigrp** | **esp** | **gre** | **icmp** | **igmp** | **ip** | **nos** | **ospf** | **pcp** | **pim** | **tcp** | **udp**} | {*source* | **addrgroup** | **any** | **host**} | {*destination* | **addrgroup** | **any** | **eq** | **gt** | **host** | **lt** | **neq** | **portgroup** | **range**} **capture session** *session*

Syntax Description

0-255	(Optional) Specifies a protocol number.
ahp	(Optional) Specifies Authentication Header Protocol.
eigrp	(Optional) Specifies Cisco's EIGRP routing protocol.
esp	(Optional) Specifies encapsulation security payload.
gre	(Optional) Specifies Cisco's GRE tunneling.
icmp	(Optional) Specifies Internet Control Message Protocol.
igmp	(Optional) Specifies Internet Group Management Protocol.
ip	(Optional) Specifies any IP protocol.
nos	(Optional) Specifies KA9Q NOS compatible IP over IP tunneling.
ospf	(Optional) Specifies OSPF routing protocol.
pcp	(Optional) Specifies Payload Compression Protocol.
pim	(Optional) Specifies protocol independent multicast.
tcp	Specifies Transport Control Protocol.
udp	(Optional) Specifies User Datagram Protocol.
source	Source network address.
addrgroup	(Optional) Specifies the source address group.
any	(Optional) Specifies any source address.
host	(Optional) Specifies a single destination host.
destination	Destination network address.
eq	(Optional) Matches only packets on a given port number.
gt	(Optional) Matches only packets with a greater port number.
lt	(Optional) Matches only packets with a lower port number.
neq	(Optional) Matches only packets not on a given port number.
portgroup	(Optional) Specifies the source port group.
range	(Optional) Matches only packets in the range of port numbers.
capture session	Specifies a capture session for the ACEs.
session	Session ID. The range is from 1 to 48.

Defaults

None

Command Modes

ACL configuration mode (config-acl)

Command History

Release	Modification
5.2(1)	This command was introduced.

Command Historyne

This command does not require a license.

Examples

This example shows how to enable a capture session for the access control entries (ACEs) of the access control list:

```
switch# configure terminal
switch(config)# ip access-list acl-1
switch(config-acl)# permit tcp host 10.1.1.1 any capture session 10
switch(config-acl)#
```

Related Commands

Command	Description
ip access-group *name* **in**	Applies an ACL with capture session ACEs to the interface.
ip access-list	Creates an access list.

permit (ARP)

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

General Syntax

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

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

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

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

no permit 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 **permit** 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	Specifies that any host matches the part of the rule that contains the **any** keyword. You can use **any** to specify the sender IP address, target IP address, sender MAC address, and target MAC address.
host *sender-IP*	Specifies that the rules 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	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 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*	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	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 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*	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	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 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*	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	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 in dotted-hexadecimal format. Specifying ffff.ffff.ffff as the *target-MAC-mask* argument is the equivalent of using the **host** keyword.

Defaults

ip

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 permits 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)# permit request ip 10.32.143.0 255.255.255.0 mac any
```

Related Commands

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

permit (IPv4)

To create an IPv4 access control list (ACL) rule that permits traffic matching its conditions, use the **permit** command. To remove a rule, use the **no** form of this command.

General Syntax

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

no permit *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*] **permit 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*] **permit 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*] **permit 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*] **permit 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*] **permit 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 **permit** 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 protocol • 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. Use the **time-range** command to a time range.
icmp-message	(ICMP only: Optional) ICMP message that the rule matches. This argument can be 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 objects.
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 *operator packet-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.

Defaults

A newly created IPv4 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.

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 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:

- 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)# permit 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)# permit 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)# permit 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)# permit 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**—Timestamp replies
- **timestamp-request**—Timestamp 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 permitting all TCP and UDP traffic from the 10.23.0.0 and 192.168.37.0 networks to the 10.176.0.0 network:

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

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

```
switch# config t
switch(config)# ip access-list acl-eng-to-marketing
switch(config-acl)# permit ip addrgroup eng_workstations addrgroup marketing_group
```

Related Commands

Command	Description
deny (IPv4)	Configures a deny rule in an IPv4 ACL.
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.
remark	Configures a remark in an 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.

permit (IPv6)

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

General Syntax

[*sequence-number*] **permit** *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 permit *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**] **permit 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*] **permit 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**] **permit 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*] **permit 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**] **permit 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 **permit** 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: • Whether the protocol was TCP, UDP, ICMP or a number protocol • 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.
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 *operator packet-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.

Defaults

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)# permit 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)# permit 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)# permit 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 permitting 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)# permit tcp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
switch(config-ipv6-acl)# permit udp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
switch(config-ipv6-acl)# permit tcp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
switch(config-ipv6-acl)# permit 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 permits 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)# permit ipv6 addrgroup eng_ipv6 addrgroup marketing_group
```

Related Commands

Command	Description
deny (IPv6)	Configures a deny rule in an IPv6 ACL.
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.
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.

permit (MAC)

To create a MAC ACL rule that permits traffic matching its conditions, use the **permit** command. To remove a rule, use the **no** form of this command.

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

no permit *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 **permit** 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.

Defaults

None

Command Modes

MAC ACL configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

A newly created MAC ACL contains no rules.

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

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 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:

- 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)# permit 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)# permit 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-filter with a rule that permits traffic between two groups of MAC addresses:

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

Related Commands

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

permit (role-based access control list)

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

permit {**all** | **icmp** | **igmp** | **ip** | {{**tcp** | **udp**} [{**src** | **dst**} {{**eq** | **gt** | **lt** | **neq**} *port-number*} | **range** *port-number1 port-number2*}]} [**log**]

no permit {**all** | **icmp** | **igmp** | **ip** | {{**tcp** | **udp**} [{**src** | **dst**} {{**eq** | **gt** | **lt** | **neq**} *port-number*} | **range** *port-number1 port-number2*}]} [**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.
log	(Optional) Specifies that packets matching this configuration be logged.

Defaults

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 permit action to an SGACL and enable RBACL logging:

```
switch# config t
switch(config)# cts role-based access-list MySGACL
switch(config-rbacl)# permit icmp log
```

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

```
switch# config t
switch(config)# cts role-based access-list MySGACL
switch(config-rbacl)# no permit icmp log
```

Related Commands

Command	Description
cts role-based access-list	Configures Cisco TrustSec SGACLs.
deny (role-based access control list)	Configures deny actions in an SGACL.
feature cts	Enables the Cisco TrustSec feature.
show cts role-based access-list	Displays the Cisco TrustSec SGACL configuration.

permit interface

To permit interfaces for a user role interface policy, use the **permit interface** command. To deny interfaces, use the **no** form of this command.

permit interface {**ethernet** *slot*/*port*[**-** *port2*]| *interface-list*}

no permit interface

Syntax Description

ethernet *slot*/*port*	Specifies the Ethernet interface identifier.
- *port*	Last interface in a range of interfaces on a module.
interface-list	Comma-separated list of Ethernet interface identifiers.

Defaults

All interfaces

Command Modes

User role interface policy configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The **interface policy deny** command denies a user role access to all interfaces except for those that you allow with the **permit interface** command.

This command does not require a license.

Examples

This example shows how to permit a range of interfaces for a user role interface policy:

```
switch# config t
switch(config)# role name MyRole
switch(config-role)# interface policy deny
switch(config-role-interface)# permit interface ethernet 2/1 - 8
```

This example shows how to permit a list of interfaces for a user role interface policy:

```
switch# config t
switch(config)# role name MyRole
switch(config-role)# interface policy deny
switch(config-role-interface)# permit interface ethernet 1/1, ethernet 1/3, ethernet 1/5,
ethernet 1/7
```

This example shows how to deny an interface in a user role interface policy:

```
switch# config t
switch(config)# role name MyRole
switch(config-role)# interface policy deny
switch(config-role-interface)# no permit interface ethernet 2/1
```

Related Commands

Command	Description
interface policy deny	Enters interface policy configuration mode for a user role.
role name	Creates or specifies a user role and enters user role configuration mode.
show role	Displays user role information.

permit vlan

To permit VLANs for a user role VLAN policy, use the **permit vlan** command. To remove VLANs, use the **no** form of this command.

permit vlan {*vlan-id*[- *vlan-id2*] | *vlan-list*}

no permit vlan

Syntax Description

vlan-id	VLAN identifier. The range is 1-3967 and 4048-4093.
- *vlan-id2*	Last VLAN identifier in a range. The VLAN identifier must be greater than the first VLAN identifier in the range.
vlan-list	Comma-separated list of VLAN identifiers.

Defaults

All VLANs

Command Modes

User role VLAN policy configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The **vlan policy deny** command denies a user role access to all VLANs except for those that you allow with the **permit vlan** command.

This command does not require a license.

Examples

This example shows how to permit a VLAN identifier for a user role VLAN policy:

```
switch# config t
switch(config)# role name MyRole
switch(config-role)# vlan policy deny
switch(config-role-vlan)# permit vlan 8
```

This example shows how to permit a range of VLAN identifiers for a user role VLAN policy:

```
switch# config t
switch(config)# role name MyRole
switch(config-role)# vlan policy deny
switch(config-role-vlan)# permit vlan 1-8
```

This example shows how to permit a list of VLAN identifiers for a user role VLAN policy:

```
switch# config t
switch(config)# role name MyRole
switch(config-role)# vlan policy deny
switch(config-role-vlan)# permit vlan 1, 10, 12, 20
```

This example shows how to deny a VLAN from a user role VLAN policy:

```
switch# config t
switch(config)# role name MyRole
switch(config-role)# vlan policy deny
switch(config-role-vlan)# no permit vlan 2
```

Related Commands

Command	Description
vlan policy deny	Enters VLAN policy configuration mode for a user role.
role name	Creates or specifies a user role and enters user role configuration mode.
show role	Displays user role information.

permit vrf

To permit virtual routing and forwarding instances (VRFs) for a user role VRF policy, use the **permit vrf** command. To remove VRFs, use the **no** form of this command.

permit vrf *vrf-name*

no permit vrf *vrf-name*

Syntax Description

vrf-name	VRF name. The name is case sensitive.

Defaults

All VRFs

Command Modes

User role VRF policy configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The **vrf policy deny** command denies a user role access to all VRFs except for those that you allow with the **permit vrf** command.

You can repeat this command to allow more than on VRF name for the user role.

This command does not require a license.

Examples

This example shows how to permit a VRF name for a user role VRF policy:

```
switch# config t
switch(config)# role name MyRole
switch(config-role)# vrf policy deny
switch(config-role-vrf)# permit vrf management
```

This example shows how to permit a VRF name from a user role VRF policy:

```
switch# config t
switch(config)# role name MyRole
switch(config-role)# vrf policy deny
switch(config-role-vrf)# no permit vrf engineering
```

Related Commands

Command	Description
vrf policy deny	Enters VRF policy configuration mode for a user role.
role name	Creates or specifies a user role and enters user role configuration mode.
show role	Displays user role information.

platform access-list update

To configure how supervisor modules update I/O modules with changes to access control lists (ACLs), use the **platform access-list update** command. To disable atomic updates, use the **no** form of this command.

platform access-list update atomic | default-result permit}

no platform access-list update {**atomic | default-result permit**}

Syntax Description

atomic	Specifies that the device performs atomic updates, which do not disrupt traffic during the update. By default, a Cisco NX-OS device performs atomic ACL updates.
default-result permit	Specifies that, during non-atomic updates, the device permits traffic that the updated ACL applies to.

Defaults

atomic

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)	This command was deprecated and replace with the **access-list update** command.
4.0(1)	This command was introduced.

Usage Guidelines

By default, a Cisco NX-OS device performs atomic ACL updates, which do not disrupt traffic that the updated ACL applies to; however, atomic updates require that the I/O modules that receive the updates have enough available resources to store each of the updated entries in the affected ACL. After the update occurs, the additional resources used for the update are freed. If the I/O module lacks the required resources, the device generates an error message and the ACL update to the I/O module fails.

If an I/O module lacks required resources, you can disable atomic updates by using the **no platform access-list update atomic** command; however, during the brief time required for the device to remove the old ACL and implement the updated ACL, traffic that the ACL applies to is dropped by default.

If you want to permit all traffic that the updated ACL applies during a non-atomic update, use the **platform access-list update default-result permit** command.

This command does not require a license.

Examples

This example shows how disable atomic updates to ACLs:

```
switch# config t
switch(config)# no platform access-list update atomic
```

This example shows how to permit affected traffic during a non-atomic ACL update:

```
switch# config t
switch(config)# platform access-list update default-result permit
```

This example shows how to revert to the atomic update method:

```
switch# config t
switch(config)# no platform access-list update default-result permit
switch(config)# platform access-list update atomic
```

Related Commands

Command	Description
show running-config all	Displays the running configuration, including the default configuration.

platform rate-limit

To configure rate limits in packets per second on supervisor-bound traffic, use the **platform rate-limit** command. To revert to the default, use the **no** form of this command.

platform rate-limit {**access-list-log** | **copy** | **layer-2** {**port-security** | **storm-control**} | **layer-3** {**control** | **glean** | **mtu** | **multicast** {**directly-connect** | **local-groups** | **rpf-leak**} | **ttl**} | **receive**} *packets*

no platform rate-limit {**access-list-log** | **copy** | **layer-2** {**port-security** | **storm-control**} | **layer-3** {**control** | **glean** | **mtu** | **multicast** {**directly-connect** | **local-groups** | **rpf-leak**} | **ttl**} | **receive**} [*packets*]

Syntax Description

access-list-log	Specifies packets copied to the supervisor module for access list logging. The default rate is 100 packets per second.
copy	Specifies data and control packets copied to the supervisor module. The default rate is 30000 packets per second.
layer-2	Specifies Layer 2 packets rate limits.
port-security	Specifies port security packets. The default is disabled.
storm-control	Specifies storm control packets. The default is disabled.
layer-3	Specifies Layer 3 packets.
control	Specifies Layer-3 control packets. The default rate is 10000 packets per second.
glean	Specifies Layer-3 glean packets. The default rate is 100 packets per second.
mtu	Specifies Layer-3 MTU failure redirected packets. The default rate is 500 packets per second.
multicast	Specifies Layer-3 multicast packets per second.
directly-connect	Specifies directly connected multicast packets. The default rate is 10000 packets per second.
local-groups	Specifies local groups multicast packets. The default rate is 10000 packets per second.
rpf-leak	Specifies Reverse Path Forwarding (RPF) leak packets. The default rate is 500 packets per second.
ttl	Specifies Layer-3 failed time-to-live redirected packets. The default rate is 500 packets per second.
receive	Specifies packets redirected to the supervisor module. The default rate is 30000 packets per second.
packets	Number of packets per second. The range is from 1 to 33554431.

Defaults

See Syntax Description for the default rate limits.

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)	This command was deprecated and replaced with the **rate-limiter** command.
4.0(3)	Added the **port-security** keyword.
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure a rate limit for control packets:

```
switch# config t
switch(config)# platform rate-limit layer-3 control 20000
```

This example shows how to revert to the default rate limit for control packets:

```
switch# config t
switch(config)# no platform rate-limit layer-3 control
```

Related Commands

Command	Description
show running-config	Displays the running configuration.

police (policy map)

To configure policing for a class map in a control plane policy map, use the **police** command. To remove policing for a class map in a control plane policy map, use the **no** form of this command.

police [**cir**] *cir-rate* [**bps** | **gbps** | **kbps** | **mbps** | **pps**]

police [**cir**] *cir-rate* [**bps** | **gbps** | **kbps** | **mbps**] [**bc**] *burst-size* [**bytes** | **kbytes** | **mbytes** | **ms** | **packets** | **us**]

police [**cir**] *cir-rate* [**bps** | **gbps** | **kbps** | **mbps** | **pps**]
conform {**drop** | **set-cos-transmit** *cos-value* | **set-dscp-transmit** *dscp-value* | **set-prec-transmit** *prec-value* | **transmit**} [**exceed** {**drop** | **set dscp dscp table cir-markdown-map** | **transmit**}] [**violate** {**drop** | **set dscp dscp table pir-markdown-map** | **transmit**}]

police [**cir**] *cir-rate* [**bps** | **gbps** | **kbps** | **mbps** | **pps**]
pir *pir-rate* [**bps** | **gbps** | **kbps** | **mbps**] [[**be**] *extended-burst-size* [**bytes** | **kbytes** | **mbytes** | **ms** | **packets** | **us**]]

no police [**cir**] *cir-rate* [**bps** | **gbps** | **kbps** | **mbps** | **pps**]

no police [**cir**] *cir-rate* [**bps** | **gbps** | **kbps** | **mbps** | **pps**] [**bc**] *burst-size* [**bytes** | **kbytes** | **mbytes** | **ms** | **packets** | **us**]

no police [**cir**] *cir-rate* [**bps** | **gbps** | **kbps** | **mbps** | **pps**]
conform {**drop** | **set-cos-transmit** *cos-value* | **set-dscp-transmit** *dscp-value* | **set-prec-transmit** *prec-value* | **transmit**} [**exceed** {**drop** | **set dscp dscp table cir-markdown-map** | **transmit**}] [**violate** {**drop** | **set dscp dscp table pir-markdown-map** | **transmit**}]

no police [**cir**] *cir-rate* [**bps** | **gbps** | **kbps** | **mbps** | **pps**]
pir *pir-rate* [**bps** | **gbps** | **kbps** | **mbps** | **pps**] [[**be**] *extended-burst-size* [**bytes** | **kbytes** | **mbytes** | **ms** | **packets** | **us**]]

Syntax Description

cir	(Optional) Specifies the committed information rate (CIR).
cir-rate	CIR rate. The range is from 0 to 80000000000.
bps	(Optional) Specifies units for traffic rates bytes per second in bits per second.
gbps	(Optional) Specifies units for traffic rates in gigabits per second.
kbps	(Optional) Specifies units for traffic rates in kilobits per second.
mbps	(Optional) Specifies units for traffic rates in megabits per second.
pps	(Optional) Specifies units for traffic rates in packets per second.
bc	(Optional) Specifies the committed burst size.
burst-size	Committed burst size. The range is from 1 to 512000000.
bytes	(Optional) Specifies the units for a burst in bytes.
kbytes	(Optional) Specifies the units for a burst in kilobytes.
mbytes	(Optional) Specifies the units for a burst in megabytes.
ms	(Optional) Specifies the units for a burst in milliseconds.

packets	(Optional) Specifies the units for a burst in packets.
us	(Optional) Specifies the units for a burst in microseconds.
conform	Configures an action when the traffic conforms to the specified rates and bursts.
drop	Specifies the drop action.
set-cos-transmit *cos-value*	Specifies setting the class of service (CoS) value. The range is from 0 to 7.
set-dscp-transmit *dscp-value*	Specifies the differentiated services code point (DSCP) value for IPv4 and IPv6 packets. The range is from 0 to 63.
set-prec-transmit *prec-value*	Specifies the precedence value for IPv4 and IPv6 packets. The range is from 0 to 7.
transmit	Specifies the transmit action.
exceed	Configures an action when the traffic exceeds the specified rates and bursts.
set dscp dscp table cir-markdown-map	Flags the packet on the CIR markdown map.
violate	(Optional) Configures an action when the traffic violates the specified rates and bursts.
set dscp dscp table pir-markdown-map	Flags the packet on the PIR markdown map.
pir *pir-rate*	Specifies the PIR rate.
be	(Optional) Specifies the extended burst size.
extended-burst-size	Extended burst size. The range is from 1 to 512000000.

Defaults

None

Command Modes

Policy map configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You can use this command only in the default VDC.

This command does not require a license.

Examples

This example shows how to specify a control plane policy map and enter policy map configuration mode:

```
switch# config t
switch(config)# policy-map type control-plane PolicyMapA
switch(config-pmap)# class ClassMapA
switch(config-pmap-c)# police cir 2000 kbps
```

This example shows how to delete a control plane policy map:

```
switch# config t
switch(config)# policy-map type control-plane PolicyMapA
switch(config-pmap)# class ClassMapA
switch(config-pmap-c)# no police 2000 kbps
```

Related Commands

Command	Description
class (policy map)	Specifies a control plane class map for a control plane policy map and enters policy map class configuration mode.
show policy-map type control-plane	Displays configuration information for control plane policy maps.

policy

To manually configure a Cisco TrustSec authentication policy on an interface with either a Cisco TrustSec device identifier or security group tag (SGT), use the **policy** command. To revert to the default, use the **no** form of this command.

policy {**dynamic identity** *device-id* | **static** sgt *sgt-value* [**trusted**]}

no policy {**dynamic** | **static**}

Syntax Description

dynamic identity	Specifies a dynamic policy using a Cisco TrustSec device identifier.
device-id	Cisco TrustSec device identifier. The device identifier is case sensitive.
static sgt	Specifies a static policy using an SGT.
sgt-value	Cisco TrustSec SGT. The *sgt-value* is either a decimal value or a hexadecimal value in the format 0xhhhh. The decimal range is from 2 to 65519, and the hexadecimal range is from 0x2 to 0xffef.
trusted	(Optional) Specifies that the traffic coming on the interface with the SGT should not have its tag overridden.

Defaults

None

Command Modes

Cisco TrustSec manual configuration

Command History

Release	Modification
6.2(2)	Modified the *sgt-value* argument to accept decimal values.
4.0(3)	Removed the keywords and options following **dynamic** and **static** in the **no** form of this command.
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.

After using this command, you must enable and disable the interface using the **shutdown/no shutdown** command sequence for the configuration to take effect.

This command requires the Advanced Services license.

Examples

This example shows how to manually configure a dynamic Cisco TrustSec policy on an interface:

```
switch# config t
switch(config)# interface ethernet 2/3
switch(config-if)# cts manual
switch(config-if-cts-manual)# policy dynamic identity DeviceB
switch(config-if-cts-manual)# exit
```

```
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

This example shows how to remove a manually configured dynamic Cisco TrustSec policy from an interface:

```
switch# config t
switch(config)# interface ethernet 2/3
switch(config-if)# cts manual
switch(config-if-cts-manual)# no policy dynamic identity DeviceB
switch(config-if-cts-manual)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

This example shows how to manually configure a static Cisco TrustSec policy on an interface:

```
switch# config t
switch(config)# interface ethernet 2/4
switch(config-if)# cts manual
switch(config-if-cts-manual)# policy static sgt 0x100
switch(config-if-cts-manual)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

This example shows how to remove a manually configured static Cisco TrustSec policy on an interface:

```
switch# config t
switch(config)# interface ethernet 2/4
switch(config-if)# cts manual
switch(config-if-cts-manual)# no policy static sgt 0x100
switch(config-if-cts-manual)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

Related Commands

Command	Description
cts manual	Enters Cisco TrustSec manual configuration mode for an interface.
feature cts	Enables the Cisco TrustSec feature.
show cts interface	Displays the Cisco TrustSec configuration for interfaces.

policy-map type control-plane

To create or specify a control plane policy map and enter policy map configuration mode, use the **policy-map type control-plane** command. To delete a control plane policy map, use the **no** form of this command.

policy-map type control-plane *policy-map-name*

no policy-map type control-plane *policy-map-name*

Syntax Description

policy-map-name	Name of the class map. The name is alphanumeric, case sensitive, and has a maximum of 64 characters.

Defaults

None

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You can use this command only in the default VDC.

This command does not require a license.

Examples

This example shows how to specify a control plane policy map and enter policy map configuration mode:

```
switch# config t
switch(config)# policy-map type control-plane PolicyMapA
switch(config-pmap)#
```

This example shows how to delete a control plane policy map:

```
switch# config t
switch(config)# no policy-map type control-plane PolicyMapA
```

Related Commands

Command	Description
show policy-map type control-plane	Displays configuration information for control plane policy maps.

propagate-sgt

To enable SGT propagation on Layer 2 Cisco TrustSec interfaces, use the **propagate-sgt** command. To disable SGT propagation, use the **no** form of this command.

propagate-sgt

no propagate-sgt

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Global configuration

Command History

Release	Modification
6.2(10)	Support was added for F3 Series modules.
4.0(3)	This command was introduced.

Usage Guidelines

You can disable the SGT propagation feature on an interface if the peer device connected to the interface can not handle Cisco TrustSec packets tagged with an SGT.

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

After using this command, you must enable and disable the interface using the **shutdown/no shutdown** command sequence for the configuration to take effect.

This command requires the Advanced Services license.

Examples

This example shows how to disable SGT propagation:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# cts dot1x
switch(config-if-cts-dot1x)# no propagate-sgt
switch(config-if-cts-dot1x)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

This example shows how to enable SGT propagation:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# cts dot1x
switch(config-if-cts-dot1x)# propagate-sgt
switch(config-if-cts-dot1x)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

Related Commands

Command	Description
cts dot1x	Enters Cisco TrustSec 802.1X configuration mode for an interface.
feature cts	Enables the Cisco TrustSec feature.
show cts interface	Displays the Cisco TrustSec configuration for interfaces.