M Commands

This chapter describes the Cisco NX-OS security commands that begin with M.

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

SupportedUserRoles

network-admin
vdc-admin

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

SupportedUserRoles

network-admin
vdc-admin

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

SupportedUserRoles

network-admin
vdc-admin

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 on page 388.

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** | **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** | **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.
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

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
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

SupportedUserRoles

network-admin
vdc-admin

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

SupportedUserRoles

network-admin
vdc-admin

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)#
```

Command	Description
hardware 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.