Configuring MAC ACLs

This chapter contains the following sections:

Information About MAC ACLs

MAC access control lists (ACLs) are ACLs that filter traffic using information in the Layer 2 header of each packet.

Prerequisites for MAC ACLs

- You must be familiar with MAC addressing and non-IP protocols to configure MAC ACLs.
- You must be familiar with the ACL concepts presented in this document.

Guidelines and Limitations for MAC ACLs

ACLs are not supported in port channels.

Default Settings for MAC ACLs

Parameters	Default
MAC ACLs	No MAC ACLs exist by default.

Parameters	Default
ACL rules	Implicit rules apply to all ACLs.

Configuring MAC ACLs

Creating a MAC ACL

You can create a MAC ACL and add rules to it. You can also use this procedure to add the ACL to a port profile.

Before you begin

- Log in to the CLI in EXEC mode.
- Have a name to assign to the ACL that you are creating.
- Create a port profile if you want to add the ACL to it.

If you want to also add the ACL to a port profile, you must know the following:

- If you are using an existing port profile, you have already created it and you know its name.
- The interface type (Ethernet or vEthernet) and the name that you want to give the port profile if you are creating a new port profile.
- The direction of packet flow for the access list.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **mac access-list** *name*	Creates the MAC ACL and enters ACL configuration mode.
Step 3	switch(config-mac-acl)# {**permit** | **deny**} *source destination protocol*	Creates a rule in the MAC ACL. The **permit** and **deny** keywords support many ways of identifying traffic. For more information, see the *Cisco Nexus 1000VE Command Reference*.
Step 4	(Optional) switch(config-mac-acl)# **statistics per-entry**	Specifies that the device maintains global statistics for packets that match the rules in the ACL.
Step 5	(Optional) switch(config-mac-acl)# **show mac access-lists** *name*	Displays the MAC ACL configuration for verification.

	Command or Action	Purpose
Step 6	(Optional) switch(config-mac-acl)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

This example shows how to create a MAC ACL:

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# mac access-list acl-mac-01
switch(config-mac-acl)# permit 00c0.4f00.0000 0000.00ff.ffff any
switch(config-mac-acl)# statistics per-entry
switch(config-mac-acl)# show mac access-lists acl-mac-01
MAC ACL acl-mac-01
        statistics per-entry
        10 permit 00c0.4f00.0000 0000.00ff.ffff any
switch(config-mac-acl)# copy running-config startup-config
```

Changing a MAC ACL

You can change an existing MAC ACL, for example, to add or remove rules.

Use the **resequence** command to reassign sequence numbers, such as when adding rules between existing sequence numbers.

Before you begin

- Log in to the CLI in EXEC mode.
- In an existing MAC ACL, know that you cannot change existing rules.
- In an existing MAC ACL, know that you can add and remove rules.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **mac access-list** *name*	Creates the MAC ACL and enters ACL configuration mode.
Step 3	(Optional) switch(config-mac-acl)# [*sequence-number*] {**permit** | **deny**} *source destination protocol*	Creates a rule in the MAC ACL. Using a sequence number allows you to specify a position for the rule in the ACL. Without a sequence number, the rule is added to the end of the rules. The **permit** and **deny** keywords support many ways of identifying traffic. For more information, see the *Cisco Nexus 1000VE Command Reference*.

	Command or Action	Purpose
Step 4	(Optional) switch(config-mac-acl)# **no** {*sequence-number* | {**permit** | **deny**} *source destination protocol*}	Removes the rule that you specify from the MAC ACL. The **permit** and **deny** keywords support many ways of identifying traffic. For more information, see the *Cisco Nexus 1000VE Command Reference*.
Step 5	switch(config-mac-acl)# [**no**] **statistics per-entry**	Specifies that the device maintains global statistics for packets that match the rules in the ACL. The **no** option stops the device from maintaining global statistics for the ACL.
Step 6	(Optional) switch(config-mac-acl)# **show mac access-lists** *name*	Displays the MAC ACL configuration for verification.
Step 7	switch(config-mac-acl)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

This example shows how to change a MAC ACL:

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# show mac access-lists

MAC ACL acl-mac-01
        statistics per-entry
        10 permit 00c0.4f00.0000 0000.00ff.ffff any
switch(config)# mac access-list acl-mac-01
switch(config-mac-acl)# permit f866.f222.e5a6 ffff.ffff.ffff any
switch(config-mac-acl)# no 10
switch(config-mac-acl)# no statistics per-entry
switch(config-mac-acl)# end
switch# show mac access-lists

MAC ACL acl-mac-01
        20 permit f866.f222.e5a6 ffff.ffff.ffff any
switch# copy running-config startup-config
```

Removing a MAC ACL

You can remove a MAC ACL from the switch. Ensure that you know whether the ACL is applied to an interface. The switch allows you to remove ACLs that are currently applied. Removing an ACL does not affect the configuration of interfaces where the ACL is applied. Instead, the switch considers the removed ACL to be empty.

To find the interfaces that a MAC ACL is configured on, use the **show mac access-lists** command with the summary keyword.

Before you begin

- Log in to the CLI in EXEC mode.
- Know whether the ACL is applied to an interface.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **no mac access-list** *name*	Removes the specified MAC ACL from the running configuration.
Step 3	(Optional) switch(config)# **show mac access-lists** *name* **summary**	Displays the MAC ACL configuration. If the ACL remains applied to an interface, the command lists the interfaces.
Step 4	(Optional) switch(config)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

This example shows how to remove a MAC ACL:

```
switch# configure terminal
switch(config)# no mac access-list acl-mac-01
switch(config)# show mac access-lists acl-mac-01 summary
switch(config)# copy running-config startup-config
```

Changing Sequence Numbers in a MAC ACL

You can change sequence numbers assigned to rules in a MAC ACL. Resequencing is useful when you need to insert rules into an ACL and there are not enough available sequence numbers.

Before you begin

Log in to the CLI in EXEC mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **resequence mac access-list** *name starting-sequence-number increment*	Assigns sequence numbers to the rules contained in the ACL, where the first rule receives the number specified by the starting-sequence number that you specify. Each subsequent rule receives a number larger than the preceding rule. The difference in numbers

	Command or Action	Purpose
		is determined by the increment number that you specify.
Step 3	(Optional) switch(config-mac-acl)# **show mac access-lists** *name*	Displays the MAC ACL configuration for verification.
Step 4	(Optional) switch(config)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

This example shows how to change sequence numbers in a MAC ACL:

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# show mac access-lists acl-mac-01
MAC ACL acl-mac-01
        10 permit 00c0.4f00.0000 0000.00ff.ffff any
        20 permit f866.f222.e5a6 ffff.ffff.ffff any
switch(config)# resequence mac access-list acl-mac-01 100 10
switch(config)# show mac access-lists acl-mac-01
MAC ACL acl-mac-01
        100 permit 00c0.4f00.0000 0000.00ff.ffff any
        110 permit f866.f222.e5a6 ffff.ffff.ffff any
switch(config)# copy running-config startup-config
```

Applying a MAC ACL as a Port ACL

You can apply a MAC ACL as a port ACL to any of the following interface types:

- Physical Ethernet interfaces
- Virtual Ethernet interfaces

A MAC ACL can also be applied to a port profile that is attached to a physical Ethernet interface or a virtual Ethernet interface.

Note ACLs cannot be applied on a port-channel interface. However, an ACL can be applied on a physical Ethernet interface that is not part of the port channel.

Before you begin

- Log in to the CLI in EXEC mode.
- Know that the ACL that you want to apply exists and is configured to filter traffic in the manner that you need for this application.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface** { **ethernet** ¦ **vethernet** } *port*	Places you into interface configuration mode for the specified interface.
Step 3	switch(config-if)# **mac port access-group** *access-list* [**in** | **out**]	Applies a MAC ACL to the interface.
Step 4	(Optional) switch(config-if)# **show running-config aclmgr**	Displays the ACL configuration.
Step 5	(Optional) switch(config-if)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

This example shows how to apply a MAC ACL as a port ACL:

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# interface vethernet 1
switch(config-if)# mac port access-group acl-mac-01 in
switch(config-if)# show running-config aclmgr
mac access-list acl-mac-01
  100 permit 00C0.4F00.0000 0000.00FF.FFFF any
  110 permit F866.F222.E5A6 FFFF.FFFF.FFFF any
interface Vethernet1
  mac port access-group acl-mac-01 in
switch(config-if)# copy running-config startup-config
```

Adding a MAC ACL to a Port Profile

You can add a MAC ACL to a port profile.

Before you begin

- Log in to the CLI in EXEC mode.
- Create the MAC ACL to add to this port profile and know its name.
- If you are using an existing port profile, know its name.
- If you are creating a new port profile, know the interface type (Ethernet or vEthernet) and the name you want to give the profile.
- Know the direction of packet flow for the access list.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **port-profile** [**type** {**ethernet** | **vethernet**}] *name*	Places you in port profile configuration mode for the named port profile.
Step 3	switch(config-port-prof)# **mac port access-group** *name* {**in** | **out**}	Adds the named ACL to the port profile for either inbound or outbound traffic.
Step 4	(Optional) switch(config-port-prof)# **show port-profile name** *profile-name*	Displays the configuration for verification.
Step 5	(Optional) switch(config-port-prof)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

This example shows how to add a MAC ACL to a port profile:

```
switch# configure termnal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# port-profile vm_eth1
switch(config-port-prof)# mac port access-group acl-mac-01 out
switch(config-port-prof)# show port-profile name vm_eth1
port-profile vm_eth1
 type: Vethernet
 description:
 status: enabled
 max-ports: 32
 min-ports: 1
 inherit:
 config attributes:
  mac port access-group acl-mac-01 out
  no shutdown
 evaluated config attributes:
  mac port access-group acl-mac-01 out
  no shutdown
 assigned interfaces:
 port-group: vm_eth1
 system vlans: none
 capability l3control: no
 capability iscsi-multipath: no
 capability vxlan: no
 capability l3-vn-service: no
 port-profile role: none
 port-binding: static

switch(config-port-prof)# copy running-config startup-config
```

Verifying MAC ACL Configurations

Use one of the following commands to verify the configuration:

Command	Purpose
show mac access-lists	Displays the MAC ACL configuration.
show running-config aclmgr	Displays the ACL configuration, including MAC ACLs and the interfaces that they are applied to.
show running-config interface	Displays the configuration of the interface to which you applied the ACL.
show mac access-lists summary	Displays a summary of all configured MAC ACLs or a named MAC ACLs.

Monitoring MAC ACLs

Use the following commands for MAC ACL monitoring:

Command	Purpose
show mac access-lists	Displays the MAC ACL configuration. If the MAC ACL includes the **statistics per-entry** command, the **show mac access-lists** command output includes the number of packets that have matched each rule.
clear mac access-list counters	Clears statistics for all MAC ACLs or for a specific MAC ACL.

Configuration Examples for MAC ACLs

Configuration Example for Creating a MAC ACL for any Protocol

This example shows how to create an MAC ACL named acl-mac-01 and apply it as a port ACL on physical ethernet interface which is not a member of port-channel and configuration verification with match counters.

```
switch(config)# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# mac access-list acl-mac-01
switch(config-mac-acl)# 100 permit 00c0.4f00.0000 0000.00ff.ffff any
switch(config-mac-acl)# 110 permit f866.f222.e5a6 ffff.ffff.ffff any
switch(config-mac-acl)# statistics per-entry
switch(config-mac-acl)# end
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# interface ethernet 3/5
switch(config-if)# mac port access-group acl-mac-01 out
switch(config-if)# show mac access-lists acl-mac-01 summary

MAC ACL acl-mac-01
        statistics per-entry
        Total ACEs Configured:2
        Configured on interfaces:
```

```
                Ethernet3/5 -  egress (Port ACL)
        Active on interfaces:
                Ethernet3/5 -  egress (Port ACL)
switch(config-if)# show mac access-lists acl-mac-01

MAC ACL acl-mac-01
        statistics per-entry
        100 permit 00c0.4f00.0000 0000.00ff.ffff any [match=0]
        110 permit f866.f222.e5a6 ffff.ffff.ffff any [match=546]
switch(config-if)# clear mac access-list counters
switch(config-if)# show mac access-lists acl-mac-01

MAC ACL acl-mac-01
        statistics per-entry
        100 permit 00c0.4f00.0000 0000.00ff.ffff any [match=0]
        110 permit f866.f222.e5a6 ffff.ffff.ffff any [match=0]
switch(config-if)#
```