Configuring MAC ACLs

This chapter describes how to configure MAC access lists (ACLs) on Cisco NX-OS devices.

This chapter contains the following sections:

About MAC ACLs

MAC ACLs are ACLs that use information in the Layer 2 header of packets to filter traffic. MAC ACLs share many fundamental concepts with IP ACLs, including support for virtualization.

MAC Packet Classification

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.

MAC Packet Classification State	Effect on Interface
Enabled	• A MAC ACL that is on the interface applies to all traffic entering the interface, including IP traffic. • You cannot apply an IP port ACL on the interface.
Disabled	• A MAC ACL that is on the interface applies only to non-IP traffic entering the interface. • You can apply an IP port ACL on the interface

Guidelines and Limitations for MAC ACLs

MAC ACLs have the following configuration guidelines and limitations:

- MAC ACLs apply to ingress traffic only.
- If you try to apply too many ACL entries, the configuration might be rejected.
- MAC packet classification is not supported when a MAC ACL is applied as part of a VACL.
- MAC packet classification is not supported when MAC ACLs are used as match criteria for QoS policies on Cisco Nexus 9300 Series switch 40G uplink ports.
- When you define a MAC ACL on the non EX/FX Cisco Nexus 9000 Series switches, you must define the ethertype for the traffic to be appropriately matched.
- Ethertype is required to match MAC ACL for EX/FX Cisco Nexus 9000 Series switches.
- Mac-packet classify knob is partially supported on the Cisco Nexus 9300-EX platform switches. In the absence of a direct field for marking the packet as an L2 packet, the switches match all packets with certain fields, such as src_mac, dst_mac, and vlan in the key field. However, they cannot match on the eth_type field. Therefore, if you install two rules with identical fields, except the MAC protocol number field, then the match conditions will remain identical in the hardware. Hence, although the first entry in the rule sequence will hit for all the packets for all the protocol numbers, the MAC protocol number will be a no-op when the mac-packet classify is configured.
- When you set a user-defined MAC limit using the **mac address-table limit <16-256> user-defined** command, the FHRP group limit is automatically adjusted to make the total user defined MAC limits and the FHRP limits to 490. For example, if you set the user dfefined MAC limit as 100, the FHRP limit gets reduced to 390.
- Beginning Cisco NX-OS Release 9.3(2), you can configure a user-defined MAC address limit between the range of 16–256.
- Cisco Nexus 93600CD-GX switches do not support breakout on port 1/1-24.
- A MAC access list applied to an interface will not block Bridge Protocol Data Unit (BPDU) traffic, such as Spanning Tree Protocol BPDUs.

Default Settings for MAC ACLs

This table lists the default settings for MAC ACL parameters.

Table 1: Default MAC ACLs Parameters

Parameters	Default
MAC ACLs	No MAC ACLs exist by 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.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**mac access-list** *name*
	Example:
	`switch(config)# mac access-list acl-mac-01`
	`switch(config-mac-acl)#`
		Creates the MAC ACL and enters ACL configuration mode.

Step 3	{**permit** | **deny**} *source destination-protocol* **Example:** `switch(config-mac-acl)# 100 permit mac 00c0.4f00.0000 0000.00ff.ffff any 0x0806`	Creates a rule in the MAC ACL. The **permit** and **deny** commands support many ways of identifying traffic.
Step 4	(Optional) **statistics per-entry** **Example:** `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) **show mac access-lists** *name* **Example:** `switch(config-mac-acl)# show mac access-lists acl-mac-01`	Displays the MAC ACL configuration.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config-mac-acl)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring a UDF-Based MAC ACL

You can configure UDF-based MAC access lists (ACLs) for the Cisco Nexus 9200, 9300, and 9300-EX Series switches. This feature enables the device to match on user-defined fields (UDFs) and to apply the matching packets to MAC ACLs.

Beginning Cisco NX-OS Release 9.3(3), you can configure UDF-based MAC access lists (ACLs) on Cisco Nexus 9364C-GX, Cisco Nexus 9316D-GX, and Cisco Nexus 93600CD-GX switches.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**udf** *udf-name offset-base offset length* **Example:** `switch(config)# udf pktoff10 packet-start 10 2`	Defines the UDF as follows: • *udf-name*—Specifies the name of the UDF. You can enter up to 16 alphanumeric characters for the name. • *offset-base*—Specifies the UDF offset base as follows: {**packet-start**}. • *offset*—Specifies the number of bytes offset from the offset base. • *length*—Specifies the number of bytes from the offset. Only 1 or 2 bytes are supported. To match additional bytes, you must define multiple UDFs. You can define multiple UDFs, but Cisco recommends defining only required UDFs.
Step 3	**hardware access-list tcam region ing-ifacl qualify** {**udf** *udf-name* } **Example:** `switch(config)# hardware access-list tcam region ing-ifacl qualify udf pktoff10`	Attaches the UDFs to the ing-ifacl TCAM region, which applies to IPv4 or IPv6 port ACLs. Up to 18 UDFs are supported.

	Command or Action	Purpose
		Note When the UDF qualifier is added, the TCAM region goes from single wide to double wide. Make sure enough free space is available; otherwise, this command will be rejected. If necessary, you can reduce the TCAM space from unused regions and then re-enter this command. For more information, see Configuring ACL TCAM Region Sizes. **Note** The **no** form of this command detaches the UDFs from the TCAM region and returns the region to single wide.
Step 4	Required: **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.
Step 5	Required: **reload** **Example:** `switch(config)# reload`	Reloads the device. **Note** Your UDF configuration is effective only after you enter **copy running-config startup-config** + **reload**.

Step 6	**mac access-list** *udf-acl*
	Example:
	`switch(config)# mac access-list udfacl`
	`switch(config-acl)#`
		Creates a MAC access control list (ACL) and enters MAC ACL configuration mode.

Step 7	**permit mac** *source destination* **udf** *udf-name value mask* **Example:** `switch(config-acl)# permit mac any any udf pktoff10 0x1234 0xffff`	Configures the MAC ACL to match on UDFs along with the current access control entries (ACEs) for the outer packet fields (example 2). The range for the *value* and *mask* arguments is from 0x0 to 0xffff. A single ACL can have ACEs with and without UDFs together. Each ACE can have different UDF fields to match, or all ACEs can match for the same list of UDFs.
Step 8	**interface port-channel** *channel-number* **Example:**	Enters interface configuration mode for a Layer 2 port-channel interface.

	Command or Action	Purpose
	`switch(config)# interface port-channel 5` `switch(config-if)#`	
Step 9	**mac port access-group** *udf-access-list* **Example:** `switch(config-if)# mac port access-group udf-acl-01`	Applies the UDF-based MAC ACL to the interface.
Step 10	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Changing a MAC ACL

You can remove a MAC ACL from the device.

Before you begin

Use the **show mac access-lists** command with the **summary** keyword to find the interfaces on which a MAC ACL is configured.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**mac access-list** *name*
	Example:
	`switch(config)# mac access-list acl-mac-01`
	`switch(config-mac-acl)#`
		Enters ACL configuration mode for the ACL that you specify by name.

Step 3	(Optional) [*sequence-number*] {**permit** | **deny**} *source destination-protocol* **Example:** `switch(config-mac-acl)# 100 permit mac 00c0.4f00.0000 0000.00ff.ffff any 0x0806`	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** commands support many ways of identifying traffic.
Step 4	(Optional) **no** {*sequence-number* | {**permit** | **deny**} *source destination-protocol*}	Removes the rule that you specify from the MAC ACL.

	Command or Action	Purpose
	Example: `switch(config-mac-acl)# no 80`	The **permit** and **deny** commands support many ways of identifying traffic.
Step 5	(Optional) [**no**] **statistics per-entry** **Example:** `switch(config-mac-acl)# 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) **show mac access-lists** *name* **Example:** `switch(config-mac-acl)# show mac access-lists acl-mac-01`	Displays the MAC ACL configuration.
Step 7	(Optional) **copy running-config startup-config** **Example:** `switch(config-mac-acl)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Changing Sequence Numbers in a MAC ACL

You can change all the 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.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**resequence mac access-list** *name starting-sequence-number increment* **Example:** `switch(config)# resequence mac access-list acl-mac-01 100 10`	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 is determined by the increment number that you specify.
Step 3	(Optional) **show mac access-lists** *name* **Example:** `switch(config)# show mac access-lists acl-mac-01`	Displays the MAC ACL configuration.

	Command or Action	Purpose
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Removing a MAC ACL

You can remove a MAC ACL from the device.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**no mac access-list** *name*
	Example:
	`switch(config)# no mac access-list acl-mac-01`
	`switch(config)#`
		Removes the MAC ACL that you specify by name from the running configuration.

Step 3	(Optional) **show mac access-lists** *name* **summary** **Example:** `switch(config)# show mac access-lists acl-mac-01 summary`	Displays the MAC ACL configuration. If the ACL remains applied to an interface, the command lists the interfaces.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

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:

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

Before you begin

Ensure 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	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	Enter one of the following commands:
	• **interface ethernet** *slot*/*port*
	• **interface port-channel** *channel-number*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
	Example:
	`switch(config)# interface port-channel 5`
	`switch(config-if)#`
		• Enters interface configuration mode for a Layer 2 or Layer 3 interface.
		• Enters interface configuration mode for a Layer 2 or Layer 3 port-channel interface.

Step 3	**mac port access-group** *access-list* **Example:** `switch(config-if)# mac port access-group acl-01`	Applies a MAC ACL to the interface.
Step 4	(Optional) **show running-config aclmgr** **Example:** `switch(config-if)# show running-config aclmgr`	Displays the ACL configuration.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Applying a MAC ACL as a VACL

You can apply a MAC ACL as a VACL.

Enabling or Disabling MAC Packet Classification

You can enable or disable MAC packet classification on a Layer 2 interface.

Before you begin

The interface must be configured as a Layer 2 interface.

Note If the interface is configured with the **ip port access-group** command or the **ipv6 port traffic-filter** command, you cannot enable MAC packet classification until you remove the **ip port access-group** and **ipv6 port traffic-filter** commands from the interface configuration.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	Enter one of the following commands:
	• **interface ethernet** *slot*/*port*
	• **interface port-channel** *channel-number*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
	Example:
	`switch(config)# interface port-channel 5`
	`switch(config-if)#`
		• Enters interface configuration mode for an Ethernet interface.
		• Enters interface configuration mode for a port-channel interface.

Step 3	[**no**] **mac packet-classify** **Example:** `switch(config-if)# mac packet-classify`	Enables MAC packet classification on the interface. The **no** option disables MAC packet classification on the interface.

Step 4	(Optional) Enter one of the following commands:
	• **show running-config interface ethernet** *slot*/*port*
	• **show running-config interface port-channel** *channel-number*
	Example:
	`switch(config-if)# show running-config interface ethernet 2/1`
	Example:
	`switch(config-if)# show running-config interface port-channel 5`
		• Displays the running configuration of the Ethernet interface.
		• Displays the running configuration of the port-channel interface.

	Command or Action	Purpose
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Verifying the MAC ACL Configuration

To display MAC ACL configuration information, perform one of the following tasks:

Command	Purpose
show mac access-lists	Displays the MAC ACL configuration.
show running-config aclmgr [**all**]	Displays the ACL configuration, including MAC ACLs and the interfaces to which MAC ACLs are applied. **Note** This command displays the user-configured ACLs in the running configuration. The **all** option displays both the default (CoPP-configured) and user-configured ACLs in the running configuration.
show startup-config aclmgr [**all**]	Displays the ACL startup configuration. **Note** This command displays the user-configured ACLs in the startup configuration. The **all** option displays both the default (CoPP-configured) and user-configured ACLs in the startup configuration.

Monitoring and Clearing MAC ACL Statistics

To monitor or clear MAC ACL statistics, use one of the commands in this table.

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 MAC ACLs.

Configuration Example for MAC ACLs

The following example shows how to create a MAC ACL named acl-mac-01 and apply it to Ethernet interface 2/1, which is a Layer 2 interface in this example:

```
mac access-list acl-mac-01
  permit 00c0.4f00.0000 0000.00ff.ffff any 0x0806
interface ethernet 2/1
  mac port access-group acl-mac-01
```

Additional References for MAC ACLs

Related Documents

Related Topic	Document Title
TAP aggregation	Configuring TAP Aggregation and MPLS Stripping