



CHAPTER 11

Configuring MAC ACLs

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

This chapter includes the following sections:

- [Information About MAC ACLs, page 11-1](#)
 - [Licensing Requirements for MAC ACLs, page 11-1](#)
 - [Prerequisites for MAC ACLs, page 11-2](#)
 - [Guidelines and Limitations, page 11-2](#)
 - [Configuring MAC ACLs, page 11-2](#)
 - [Verifying MAC ACL Configurations, page 11-8](#)
 - [Displaying and Clearing MAC ACL Statistics, page 11-8](#)
 - [Example Configuration for MAC ACLs, page 11-9](#)
 - [Default Settings, page 11-9](#)
 - [Additional References, page 11-9](#)

Information About MAC ACLs

MAC ACLs are ACLs that filter traffic using information in the Layer 2 header of each packet. MAC ACLs share many fundamental concepts with IP ACLs, including support for virtualization. For information about these shared concepts, see the [“Information About ACLs” section on page 10-1](#).

Licensing Requirements for MAC ACLs

Product	License Requirement
	<i>Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 4.0</i>

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 concepts in the [“Information About ACLs”](#) section on page 10-1.

Guidelines and Limitations

-
- ACL statistics are not supported if the DHCP snooping feature is enabled.

Configuring MAC ACLs

-
- [, page 11-3](#)
- [Removing a MAC ACL, page 11-5](#)
- [Changing Sequence Numbers in a MAC ACL, page 11-6](#)
- [Applying a MAC ACL as a Port ACL, page 11-6](#)
- [Applying a MAC ACL as a VACL, page 11-8](#)

Creating a MAC ACL

BEFORE YOU BEGIN

[switchto vdc](#) command). Because ACL names can be repeated in different VDCs, we recommend that you confirm which VDC you are working in.

SUMMARY STEPS

1. `config t`
2. `mac access-list name`
3. `{permit | deny} destination protocol`
- 4.
- 5.
6. `copy running-config startup-config`

DETAILED STEPS

	Command	Purpose
Step 1	<code>config t</code>	
	Example: switch# config t switch(config)#	
	<code>access-list name</code>	
	switch(config)# mac access-list acl-mac-01 switch(config-mac-acl)#	
	{ permit deny } source destination protocol switch(config-mac-acl)# permit 00c0.4f00.0000 0000.00ff.ffff any	<i>Cisco Nexus 7000 Series NX-OS Security Command Reference, Release 4.0</i>
<code>show mac access-lists</code>		
Example:		
<code>copy running-config startup-config</code>		
Example: running-config startup-config		

Changing a MAC ACL

resequence

BEFORE YOU BEGIN

switchto vdc

SUMMARY STEPS

1. config t
2. mac access-list

```
[sequence-number] {          } source destination protocol
    {sequence-number | {          }
[ ]
```

7.

DETAILED STEPS

	Command	Purpose
Step 1		
Step 2		
Step 3	<pre>[sequence-number] { } source destination protocol switch(config-mac-acl)# 100 permit mac 00c0.4f00.00 0000.00ff.ffff any</pre>	<p>(Optional) 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.</p> <p>The <code>permit</code> and <code>deny</code> commands support many ways of identifying traffic. For more information, see the ACL Configuration chapter.</p>
	<pre>switch(config-mac-acl)# no 80</pre>	<p>(Optional) Removes the rule that you specify from the MAC ACL.</p> <p>The <code>permit</code> and <code>deny</code> commands support many ways of identifying traffic. For more information, see the ACL Configuration chapter.</p>
	<pre>[] switch(config-mac-acl)# statistics per-entry</pre>	<p>(Optional) Specifies that the device maintains global statistics for packets that match the rules in the ACL.</p> <p>The <code>no</code> option stops the device from maintaining global statistics for the ACL.</p>
	<pre>switch(config-mac-acl)# show mac access-lists acl-mac-01</pre>	<p>(Optional) Displays the MAC ACL configuration.</p>
	<pre>switch(config-mac-acl)# copy running-config startup-config</pre>	<p>(Optional) Copies the running configuration to the startup configuration.</p>

Removing a MAC ACL

BEFORE YOU BEGIN

SUMMARY STEPS

- 1.
- 2.
- 3.
- 4.

DETAILED STEPS

	Command	Purpose
Step 1		
Step 2		
Step 3		
Step 4		

Changing Sequence Numbers in a MAC ACL

BEFORE YOU BEGIN

SUMMARY STEPS

- 1.
- 2.
- 3.
- 4.

DETAILED STEPS

	Command	Purpose
Step 1		
Step 2	<pre> resequence mac access-list <i>starting-sequence-number increment</i> switch(config)# resequence mac access-list acl-mac-01 100 10 </pre>	
	<pre> switch(config)# show mac access-lists acl-mac-01 </pre>	
	<pre> switch(config)# copy running-config startup-config </pre>	

Applying a MAC ACL as a Port ACL

-
-

/
channel-number
access-list

/	
switch(config)# interface ethernet 2/1 switch(config-if)#	
<i>channel-number</i>	
switch(config)# interface port-channel 5 switch(config-if)#	
switch(config-if)# mac port access-group acl-01	
switch(config-if)# show running-config aclmgr	
switch(config-if)# copy running-config startup-config	

Applying a MAC ACL as a VACL

Verifying MAC ACL Configurations

Command	Purpose

Displaying and Clearing MAC ACL Statistics

Command	Purpose

Example Configuration for MAC ACLs

Default Settings

Table 11-1 Default MAC ACLs Parameters

	Default

Additional References

-
-

Related Documents

Related Topic	Document Title
	Information About ACLs, page 10-1
	<i>Cisco Nexus 7000 Series NX-OS Security Command Reference, Release 4.0</i>

Standards

Standards	Title
	—

