



Configuring IP ACLs

This chapter describes how to configure IP access control lists (ACLs) on NX-OS devices. Unless otherwise specified, the term IP ACL refers to IPv4 and IPv6 ACLs.



Note

Although we fully support IPv6 ACLs, we recommend that you perform thorough validation testing of your IPv6 ACL implementation prior to deploying it in a production environment

- [Information About ACLs, page 1](#)
- [This is TopicHead level 1, page 2](#)
- [Policy-Based ACLs, page 5](#)
- [This is TopicHead Level 1, page 6](#)
- [Example Configuration for IP ACLs, page 13](#)

Information About ACLs

An ACL is an ordered set of rules that you can use to filter traffic. Each rule specifies a set of conditions that a packet must satisfy to match the rule. When the device determines that an ACL applies to a packet, it tests the packet against the conditions of all rules. The first matching rule determines whether the packet is permitted or denied. If there is no match, the device applies the applicable default rule. The device continues processing packets that are permitted and drops packets that are denied. For more information, see the [Order of ACL Application with Figures, on page 1](#)

This Section includes the following Topics

- [About Rules and indexes and conref tests republish 1, on page 2](#)
- [Order of ACL Application with Figures, on page 1](#)

Order of ACL Application with Figures

When the device processes a packet, it determines the forwarding path of the packet. The path determines which ACLs that the device applies to the traffic. The device applies the ACLs in the following order:

- 1 Port ACL
- 2 Ingress VACL
- 3 Ingress router ACL
- 4 SGACL
- 5 Egress router ACL
- 6 Egress VACL

If the packet is bridged within the ingress VLAN, the device does not apply router ACLs.

The Following figure shows the order in which the device applies ACLS.

Figure 1: Order of ACL Application

The following figure shows where the device applies ACLs, depending upon the type of ACL. The red path indicates a packet sent to a destination on a different interface than its source. The blue path indicates a packet that is bridged within its VLAN.

Figure 2: ACLs and Packet Flow

This is TopicHead level 1

About Rules and indexes and conref tests republish 1

Rules are what you create, modify, and remove when you configure how an ACL filters network traffic. Rules appear in the running configuration. When you apply an ACL to an interface or change a rule within an ACL that is already applied to an interface, the supervisor module creates ACL entries from the rules in the running configuration and sends those ACL entries to the applicable I/O module. Depending upon how you configure the ACL, there may be more ACL entries than rules, especially if you use object groups when you configure rules. For more information, see the

Imagetest edition

imagetest conref Cisco Unified IP Phone [Table 5: MIBs, on page 12](#)

Imagetest edit in XMEE bridge

You can create rules in ACLs and tYou can create rules in access-list configuration mode by using the **permit** or **deny** command. The device allows traffic that matches the criteria in a permit rule and blocks traffic that matches the criteria in a deny rule. You have many options for configuring the criteria that traffic must meet in order to match the rule

QA: FSCR01-40-2 test that this conref table appears

QA Test CSCsw88625 This description should appear before the table title in BOTH html and PDF renditions. Previously this was getting concatenated with the table title

Table 1: Table title

Product	License Requirement
NX-OS	AAA requires no license. Cisco Unified MeetingPlace Cisco Unified MeetingPlace web meeting room Any feature not included in a license package is bundled with the Cisco NX-OS system images and is Cisco Unified MeetingPlace Cisco Unified MeetingPlace web meeting room provided at no extra charge to you. For a complete explanation of the NX-OS licensing scheme, see the Cisco NX-OS Licensing Guide, Release 4.0. Cisco Unified IP Phone

QA: FSCR01-20-25 The index link should be generated on the fifth level and the second level because the second level is the last index term on the policy based ACLs topic. Go to the index and look at the first index - fifth index.

This section describes some of the options that you can use when you configure a rule. For information about every option, see the applicable **permit** and **deny** commands in the *Cisco NX-OS Security Command Reference*

image here 

QA: CSCsx53724 In the next paragraph, there should be no space after the text "Cisco Unifie MeetingPlace"

and the perod that follows it. Image here 



This is Cisco Unified MeetingPlace Cisco Unified MeetingPlace web meeting room.

QA CSCsz10127 This is a xref to a step, it should render. [Step 2, on page 9](#)


QA: CSCsx83199 Check that there no no spaces before and after "command" Before command after Before **command** after

before Cisco Unified MeetingPlace Cisco Unified MeetingPlace web meeting room after

Table 2: Table for xref

table head	Desc
this is a table	for xref
image here 	image here 

QA Test: CSCtd75733. Check that the following double bytesmart quotes appear while rendering: “smart quotes”. Edit this topic (c_About_Rules.xml) and see the the double byte smart quotes appear correctly. Export

this topic and see if the double byte smart quotes are still in tact. image here 

Profiling Tests

-
-
-

-
-
-
-
-
-
-
-
-
-
-
-
-
-
-

New profile values added after phase 2

This is a simple table	blah blah blach
QA Test CSCte43613: Test that the note below appears correctly Note I am a very long note and i like ot be very very long and i dont like to runn across a table and i like messing things up and I create problems for everyone becuase i am an note in a simpletable	Note I am a very long note and i like ot be very very long and i dont like to runn across a table and i like messing things up and I create problems for everyone becuase i am an note in a simpletable

Additional Filtering Options

You can identify traffic by using additional options. These options differ by ACL type. The following list includes most but not all additional filtering options hel lo:

- IPv4 ACLs support the following additional filtering options:
 - Layer 4 protocol
 - TCP and UDP ports
 - ICMP types and codes
 - IGMP types
 - Precedence level
 - Differentiated Services Code Point (DSCP) value
 - TCP packets with the ACK, FIN, PSH, RST, SYN, or URG bit set
 - Established TCP connections
- IPv6 ACLs support the following additional filtering options:
 - Layer 4 protocol
 - Authentication Header Protocol

- Encapsulating Security Payload
 - Payload Compression Protocol
 - Stream Control Transmission Protocol (SCTP)
 - SCTP, TCP, and UDP ports
 - ICMP types and codes
 - IGMP types
 - Flow label
 - DSCP value
 - TCP packets with the ACK, FIN, PSH, RST, SYN, or URG bit set
 - Established TCP connections
- MAC ACLs support the following additional filtering options:
 - Layer 3 protocol
 - VLAN ID
 - Class of Service (CoS)

For information about all filtering options available in rules, see the applicable `permit` and `deny` commands in the *Cisco NX-OS Security Command References*

Policy-Based ACLs

The device supports policy-based ACLs (PBACLs), which allow you to apply access control policies across object groups. An object group is a group of IP addresses or a group of TCP or UDP ports. When you create a rule, you specify the object groups rather than specifying IP addresses or ports.

QA: Added by QA for check <uicontrol> font Using object groups when you configure IPv4 or IPv6 ACLs can help of updating to add or remove addresses or ports from the source or destination of rules. For example, if three rules reference the same IP address group object, rules

QA: Testing font for <ph> element PBACLs do not reduce the resources required by an ACL when you apply it to an interface. When you apply a PBACL or update a PBACL that is already applied, *QA: Added by QA for check <i> font* the device expands each rule that refers to object groups into one ACL entry per object within the group. If a rule specifies the source and destination both with object groups, the number of ACL entries created on the I/O module when you apply the PBACL is equal to the number of objects in the source group multiplied by the number of objects in the destination group **QA: Added by QA for Test element**

- QA: Testing font for <ph> element
IPv4 address object groups—Can be used with IPv4 ACLs rules to specify source or destination addresses. When you used the `permit` or `deny` command to configure a rule, the `addrgroup` keyword allows you to specify an object group for the source or destination

QA: Added by QA for check <i> font

- IPv6 address object groups—Can be used with IPv6 ACL rules to specify source or destination addresses. When you use the **permit** or **deny** command to configure a rule, the `addgroupkeyword` allows you to specify an object group for the source or destination. **QA: Added by QA for check <uicontrol> font.**

This is TopicHead Level 1

Configuring IP ACLs

This Figure shows the IPv4 ACL content

Figure 3: IPv4 ACL Content Pane

CSCsx68329: Second level bullets should look different from first level bullets

- a first level bullet
- another first level bullet
 - second level bullet

This section includes the following topics:

Task with no summary steps

You can apply an IPv4 or IPv6 ACL to a Layer 2 interface, which can be a physical port or a port channel. ACLs applied to these interface types are considered port ACLs.

QA Test: CSCsw89155 The following procedure should render without any summary steps when rendering a topic. When rendering the whole book, it may show. There is a different cdets case open to track that

Before You Begin

Ensure that the ACL you want to apply exists and that it is configured to filter traffic in the manner that you need for this application. For more information, see the or the

DETAILED STEPS

	Command or Action	Purpose
Step 1	config t Example: switch# config t switch(config)#	Enters global configuration mode.

	Command or Action	Purpose		
Step 2	interface ethernet <i>slot/port</i>	Enters interface configuration mode for a Layer 2 or Layer 3 physical interface		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>QA:CSCsu72601: This choicetable should not be dropped</td> <td>choice table description</td> </tr> </tbody> </table> <p>Example: <pre>switch(config)# interface ethernet 2/3 switch(config-if)#</pre></p>		Option	Description
Option	Description			
QA:CSCsu72601: This choicetable should not be dropped	choice table description			
Step 3	ip port access-group ipv6 port traffic-filter <i>access-list in</i> Example: <pre>switch(config-if)# ip port access-group acl-12-marketing-group in</pre>	Applies an IPv4 or IPv6 ACL to the interface or port channel. Only inbound filtering is supported with port ACLs. You can apply one port ACL to an interface.		
Step 4	show running-config aclmgr Example: <pre>switch(config-if)# show running-config aclmgr</pre>	(Optional) QA: Optional Step Test. Make sure that the word (Optional) appears Here		
Step 5	copy running-config startup-config Example: <pre>switch(config-if)# copy running-config startup-config</pre>	(Optional) Copies the running configuration to the startup configuration. CSCsy00824: This is a step result. It should render.		

QA: Added for test Example title in task

To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.

Forth Level Topic

Using object groups when you configure IPv4 or IPv6 ACLs can help reduce the complexity of updating ACLs when you need to add or remove addresses or ports from the source or destination of rules. For example, if three rules reference the same IP address group object, you can add an IP address to the object instead of changing all three rules

QA: Added for test Section titel in concept

PBACLs do not reduce the resources required by an ACL when you apply it to an interface. When you apply a PBACL or update a PBACL that is already applied, the device expands each rule that refers to object groups into one ACL entry per object within the group. If a rule specifies the source and destination both with object groups, the number of ACL entries created on the I/O module when you apply the PBACL is equal to the number of objects in the source group multiplied by the number of objects in the destination group

QA: Added for test Example title in concept

To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.

*Fifth Level References Topic***QA: Added for test Section Title in reference****Table 3: Table Title**

Product	License Requirement
NX-OS	AAA requires no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For a complete explanation of the NX-OS licensing scheme, see the Cisco NX-OS Licensing Guide, Release 4.0.

Table 4: Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/support

QA: Added for test Example Title in reference

You can apply an IPv4 or IPv6 ACL to a Layer 2 interface, which can be a physical port or a port channel. ACLs applied to these interface types are considered port ACLs.

QA: Testing font for <ph> element

Creating an IP ACL

You can create an IPv4 ACL or IPv6 ACL on the device and add rules to it.

Before You Begin

Ensure that you are in the correct VDC (or use the **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. (Optional) **config t**
2. **ipipv6access-listname**
3. *sequence-number***permitdenyprotocolsource***destination*
4. **statistics per-entry**
5. **show ip access-listsname**
6. **copy running-config startup-config**
7. Added by QA

DETAILED STEPS

Step 1 (Optional) **config t**

Example:

QA test CSCsz39546: In the above step 1, the word optional should show

```
switch# config t
switch(config)#
.
```

Enters global configuration mode.

Step 2 **ipipv6access-listname**

Example:

```
switch(config)# ip access-list acl-01
switch(config-acl)#
```

Creates the IP ACL and enters IP ACL configuration mode. The name argument can be up to 64 characters.

Step 3 *sequence-number***permitdenyprotocolsource***destination*

Example:

```
switch(config-acl)# permit ip 192.168.2.0/24 any
```

Creates a rule in the IP ACL. You can create many rules. The sequence-number argument can be a whole number between 1 and 4294967295.

The **permit** and **deny** commands support many ways of identifying traffic. For more information, see the *Cisco NX-OS Security Command Reference*

Step 4 **statistics per-entry**

Example:

```
switch(config-acl)# statistics per-entry
```

Specifies that the device maintains global statistics for packets that match the rules in the ACL.

Step 5 **show ip access-listsname**

Example:

```
switch(config-acl)# show ip access-lists acl-01
```

Displays the IP ACL configuration.

Step 6 **copy running-config startup-config**

Example:

```
switch(config-acl)# copy running-config startup-config
```

Copies the running configuration to the startup configuration.

Step 7 Added by QA

Example:

```
QA DEC-CM-36 This bold should render in yellow highlights
```

Task with No table

You can change, reorder, add, and remove rules in an existing IPv4 or IPv6 ACL. You cannot change existing rules. Instead, to change a rule, you can remove it and recreate it with the desired changes. *QA: Added by QA for check <i>font*

If you need to add more rules between existing rules than the current sequence numbering allows, you can use the *QA: check font <cmdname> for test* **resequence** command to reassign sequence numbers. For more information, see the *.QA: Added by QA for check <uicontrol> font*

Before You Begin

Ensure that you are in the correct VDC (or use the **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. *QA: Added by QA for check <uicontrol> font***QA: Added by QA for check <cmd> font****config t**
2. **ip|ipv6 access-list** *name*
3. *sequence-number* **permit|deny** *protocol source destination*
4. **no** {*sequence-number*} {**permit|deny**} *protocol source destination*
5. [**no**] **statistics per-entry**
6. **show ip access-lists** *name*
7. **copy running-config startup-config**

DETAILED STEPS

Step 1 *QA: Added by QA for check <uicontrol> font***QA: Added by QA for check <cmd> font****config t**

Example:

```
switch# config t
switch(config)#
```

Enters global configuration mode. *QA: Added by QA for check <uicontrol> font*

Step 2 **ip|ipv6 access-list** *name*

Example:

```
switch(config)# ip access-list acl-01
switch(config-acl)#
```

Enters IP ACL configuration mode for the ACL that you specify by name.

Step 3 `sequence-number permit|deny protocol source destination`

Example:

```
switch(config-acl)# 100 permit ip 192.168.2.0/24 any
```

Creates a rule in the IP 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 sequence-number argument can be a whole number between 1 and 4294967295.

The **permit** and **deny** commands support many ways of identifying traffic. *QA: Added by QA for check <i>font*For more information, see the QA: Check this is font for <cite>Cisco NX-OS Security Command Reference

Step 4 `no {sequence-number} {permit|deny} protocol source destination`

Example:

```
switch (config-acl) # no 80
```

Removes the rule that you specified from the IP ACL.

Step 5 `[no] statistics per-entry`

Example:

```
switch (config-acl) # statistics per-entry
```

Specifies that the device maintains global statistics for packets that match the rules in the ACL.

The **noQA: Added by QA for check <uicontrol> font** option stops the device from maintaining global statistics for the ACL.

Step 6 `show ip access-lists name`

Example:

```
switch (config-acl)# show ip access-lists acl-01
```

Displays the IP ACL configuration.

Step 7 `copy running-config startup-config`

Example:

```
switch (config-acl) # copy running-config startup-config
```

Copies the running configuration to the startup configuration.

Applying an ACL as a VACL

You can apply an IP ACL as a VACL. For information about how to create a VACL using an IPv4 or IPv6 ACL, see the “Creating or Changing a VACL” section on page 12-3.

Additional References

Related documents

Related Topic	Document Title
Concepts about VACLs	Example Configuration for IP ACLs, on page 13
IP ACL commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	<i>Cisco NX-OS Security Command Reference</i>
Object group commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	<i>Cisco NX-OS Security Command Reference</i>
Time range commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	<i>Cisco NX-OS Security Command Reference</i>

Standards

Standard/RFC	Title
No New or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

Table 5: MIBs

MIB	MIBs Link
This is a test for MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/support</p>

Feature History for IP ACLs

Feature Name	Releases	Feature Information
statistics	4.0(3)	The Name of the statistics command was changed to statistics bug entry
QA: DEC-CM-39 This table should render as wide		

Feature Name	Releases	Feature Information
statistics	4.0(3)	The Name of the statistics command was changed to statistics bug entry
QA: DEC-CM-39 This table should render as wide		

Example Configuration for IP ACLs**Example 1**

The following example shows how to create an IPv4 ACL named acl-01 and apply it as a port ACL to Ethernet interface 2/1, which is a Layer 2 interface:

```

ipv6 access-list acl-120
 permit tcp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
 permit udp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
 permit tcp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
 permit udp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64

```

```
interface ethernet 2/3
  ipv6 traffic-filter acl-120 in
```

Example 2

The following example shows how to create an IPv4 ACL named acl-01 and apply it as a port ACL to Ethernet interface 2/1, which is a Layer 2 interface:

```
ipv6 access-list acl-120
  permit tcp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
  permit udp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
  permit tcp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
  permit udp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
interface ethernet 2/3
  ipv6 traffic-filter acl-120 in
```

Example 3

```
ipv6 access-list acl-120
  permit tcp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
  permit udp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
  permit tcp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
  permit udp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
interface ethernet 2/3
  ipv6 traffic-filter acl-120 in
```

QA FSCR01-20-6 This is a test for figures

Figure 4: QA FSCR01-20-6 Test that the figure numbers appear in sequence

Before You Begin

This is a test for figures.

-

SUMMARY STEPS

- 1.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Example:	This Figure should appear <i>Figure 5: This is another figure</i> <i>Figure 6: QA FSCR01-20-6 Test that the figure numbers appear in sequence</i>

What to Do Next

.

Task with only one step QA FSCR01-20-37**SUMMARY STEPS**

1. QA:FSCR01-20-37 test that only summary steps are still generated

DETAILED STEPS

	Command or Action	Purpose
Step 1	QA:FSCR01-20-37 test that only summary steps are still generated Example: test	testing autogeneration of summary steps This is step result

What to Do Next

QA: FSCR01-20-50 A title what do do next should be autogenerated. Fonts should be Univers 47 condensed light. font size 13.5 pt, Bold

QA Link and URL Tests

QA: FSCR01-60-6 . Click on the following bogus Link and see if the page opens up. The Link may give you a 404 error, however the New page should open up.<http://www.ghTurk.com>

sem title

Error Message QA test: CSCsx38952 this should be in courier fonts

Explanation This is a para

Recommended Action this is a para

