



## CHAPTER 7

# 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 IPv4ACLs.

This chapter includes the following sections:

- [Information About ACLs, page 7-1](#)
- [Licensing Requirements for IP ACLs, page 7-8](#)
- [Prerequisites for IP ACLs, page 7-8](#)
- [Guidelines and Limitations, page 7-8](#)
- [Configuring IP ACLs, page 7-9](#)
- [Displaying IP ACL Statistics, page 7-13](#)
- [Field Descriptions for IPv4 ACLs, page 7-13](#)
- [Configuring Time Ranges, page 7-18](#)
- [Field Descriptions for Time Ranges, page 7-20](#)
- [Additional References, page 7-21](#)

## 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 [“Implicit Rules” section on page 7-4](#).

You can use ACLs to protect networks and specific hosts from unnecessary or unwanted traffic. For example, you could use ACLs to disallow HTTP traffic from a high-security network to the Internet. You could also use ACLs to allow HTTP traffic but only to specific sites, using the IP address of the site to identify it in an IP ACL.

This section includes the following topics:

- [ACL Types and Applications, page 7-2](#)
- [Order of ACL Application, page 7-2](#)
- [About Rules, page 7-4](#)

**[Send document comments to nexus7k-docfeedback@cisco.com.](mailto:nexus7k-docfeedback@cisco.com)**

- [Time Ranges, page 7-6](#)
- [Statistics, page 7-7](#)
- [Virtualization Support, page 7-8](#)

## ACL Types and Applications

The device supports the following types of ACLs for security traffic filtering:

- IPv4 ACLs—The device applies IPv4 ACLs only to IPv4 traffic.
- MAC ACLs—The device applies MAC ACLs only to non-IP traffic. For more information, see the [“Information About MAC ACLs” section on page 8-1](#).

IP and MAC ACLs have the following three types of applications:

- Port ACL—Filters Layer 2 traffic
- Router ACL—Filters Layer 3 traffic
- VLAN ACL—Filters VLAN traffic

[Table 7-1](#) summarizes the applications for security ACLs.

**Table 7-1 Security ACL Applications**

Application	Supported Interfaces	Types of ACLs Supported
Port ACL	<ul style="list-style-type: none"> <li>• Layer 2 interfaces</li> <li>• Layer 2 Ethernet port-channel interfaces</li> </ul> <p>When a port ACL is applied to a trunk port, the ACL filters traffic on all VLANs on the trunk port.</p>	<ul style="list-style-type: none"> <li>• IPv4 ACLs</li> <li>• MAC ACLs</li> </ul>
Router ACL	<ul style="list-style-type: none"> <li>• VLAN interfaces (sometimes referred to as switched virtual interfaces or SVIs)</li> <li>• Physical Layer 3 interfaces</li> <li>• Layer 3 Ethernet subinterfaces</li> <li>• Layer 3 Ethernet port-channel interfaces</li> <li>• Layer 3 Ethernet port-channel subinterfaces</li> <li>• Tunnels</li> <li>• Management interfaces</li> </ul>	<ul style="list-style-type: none"> <li>• IPv4 ACLs</li> </ul> <p><b>Note</b> MAC ACLs are not supported on Layer 3 interfaces.</p>
VLAN ACL	<ul style="list-style-type: none"> <li>• VLANs</li> </ul> <p>For more information about VLAN ACLs, see <a href="#">Chapter 9, “Configuring VLAN ACLs.”</a></p>	<ul style="list-style-type: none"> <li>• IPv4 ACLs</li> <li>• MAC ACLs</li> </ul>

## Order of ACL Application

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

**Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).**

3. Ingress router ACL
4. Egress router ACL
5. Egress VACL

If the packet is bridged within the ingress VLAN, the device does not apply router ACLs. Figure 7-1 shows the order in which the device applies ACLs.

**Figure 7-1 Order of ACL Application**

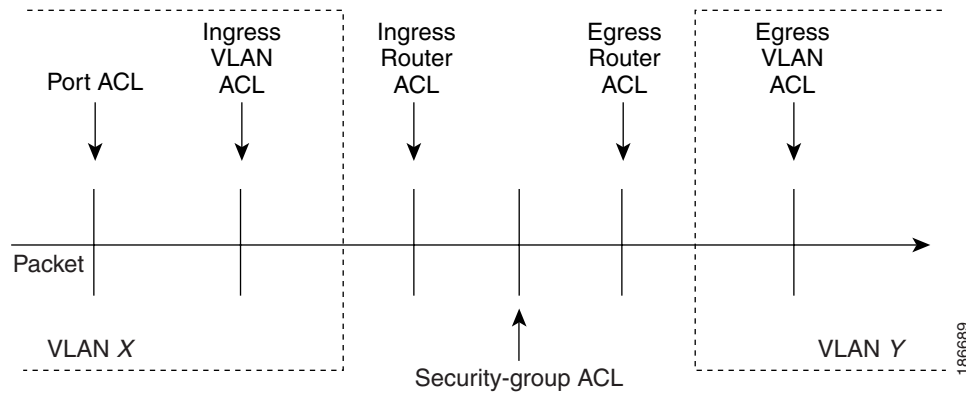
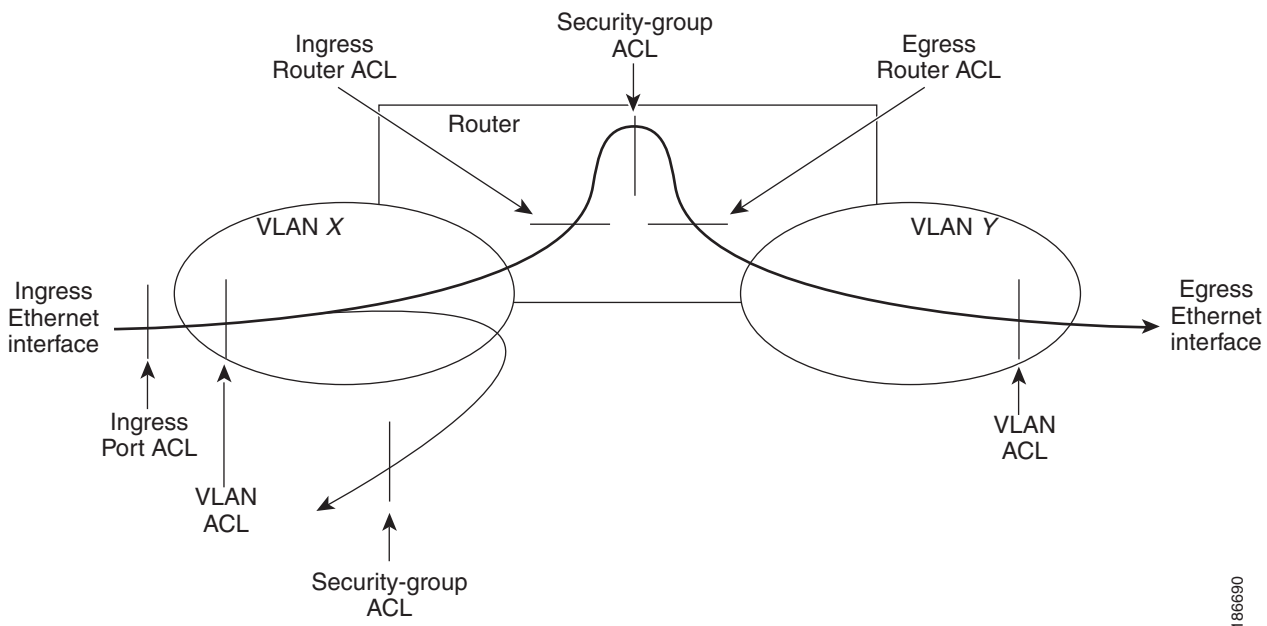


Figure 7-2 shows where the device applies ACLs, depending upon the type of ACL. The red path indicates a packet sent to a destination on a different interface than its source. The blue path indicates a packet that is bridged within its VLAN.

The device applies only the applicable ACLs. For example, if the ingress port is a Layer 2 port and the traffic is on a VLAN that is a VLAN interface, a port ACL and a router ACL both can apply. In addition, if a VACL is applied to the VLAN, the device applies that ACL too.

**Figure 7-2 ACLs and Packet Flow**



***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).***

## About Rules

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.

You can create rules in ACLs and 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.

This section describes some of the options that you can use when you configure a rule.

This section includes the following topics:

- [Source and Destination, page 7-4](#)
- [Protocols, page 7-4](#)
- [Implicit Rules, page 7-4](#)
- [Additional Filtering Options, page 7-5](#)
- [Logical Operators and Logical Operation Units, page 7-5](#)
- [Logging, page 7-6](#)

## Source and Destination

In each rule, you specify the source and the destination of the traffic that matches the rule. You can specify both the source and destination as a specific host, a network or group of hosts, or any host. How you specify the source and destination depends on whether you are configuring IPv4 or MAC ACLs.

## Protocols

IPv4 and MAC ACLs allow you to identify traffic by protocol. For your convenience, you can specify some protocols by name. For example, in an IPv4 ACL, you can specify ICMP by name.

You can specify any protocol by number. In MAC ACLs, you can specify protocols by the Ethertype number of the protocol, which is a hexadecimal number. For example, you can use 0x0800 to specify IP traffic in a MAC ACL rule.

In IPv4 ACLs, you can specify protocols by the integer that represents the Internet protocol number. For example, you can use 115 to specify Layer 2 Tunneling Protocol (L2TP) traffic.

## Implicit Rules

IP and MAC ACLs have implicit rules, which means that although these rules do not appear in the running configuration, the device applies them to traffic when no other rules in an ACL match. When you configure the device to maintain per-rule statistics for an ACL, the device does not maintain statistics for implicit rules.

All IPv4 ACLs include the following implicit rule:

```
deny ip any any
```

This implicit rule ensures that the device denies unmatched IP traffic.

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).***

All MAC ACLs include the following implicit 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.

## 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:

- 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
- MAC ACLs support the following additional filtering options:
  - Layer 3 protocol
  - VLAN ID
  - Class of Service (CoS)

## Logical Operators and Logical Operation Units

IP ACL rules for TCP and UDP traffic can use logical operators to filter traffic based on port numbers. The device stores operator-operand couples in registers called logical operator units (LOUs). Cisco Nexus 7000-series devices support 104 LOUs.

The LOU usage for each type of operator is as follows:

- eq—Is never stored in an LOU
- gt—Uses 1/2 LOU
- lt—Uses 1/2 LOU
- neq—Uses 1/2 LOU
- range—Uses 1 LOU

The following guidelines determine when the devices store operator-operand couples in LOUs:

- If the operator or operand differs from other operator-operand couples that are used in other rules, the couple is stored in an LOU.

For example, the operator-operand couples “gt 10” and “gt 11” would be stored separately in half an LOU each. The couples “gt 10” and “lt 10” would also be stored separately.

## ***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).***

- Whether the operator-operand couple is applied to a source port or a destination port in the rule affects LOU usage. Identical couples are stored separately when one of the identical couples is applied to a source port and the other couple is applied to a destination port.

For example, if a rule applies the operator-operand couple “gt 10” to a source port and another rule applies a “gt 10” couple to a destination port, both couples would also be stored in half an LOU, resulting in the use of one whole LOU. Any additional rules using a “gt 10” couple would not result in further LOU usage.

## Logging

You can enable the device to create an informational log message for packets that match a rule. The log message contains the following information about the packet:

- Protocol
- Status of whether the packet is a TCP, UDP, or ICMP packet, or if the packet is only a numbered packet.
- Source and destination address
- Source and destination port numbers, if applicable

## Time Ranges

You can use time ranges to control when an ACL rule is in effect. For example, if the device determines that a particular ACL applies to traffic arriving on an interface, and a rule in the ACL uses a time range that is not in effect, the device does not compare the traffic to that rule. The device evaluates time ranges based on its clock.

When you apply an ACL that uses time ranges, the device updates the affected I/O module whenever a time range referenced in the ACL starts or ends. Updates that are initiated by time ranges occur on a best-effort priority. If the device is especially busy when a time range causes an update, the device may delay the update by up to a few seconds.

IPv4 and MAC ACLs support time ranges. When the device applies an ACL to traffic, the rules in effect are as follows:

- All rules without a time range specified
- Rules with a time range that includes the second when the device applies the ACL to traffic.

The device supports named, reusable time ranges, which allows you to configure a time range once and specify it by name when you configure many ACL rules. Time range names have a maximum length of 64 alphanumeric characters.

A time range contains one or more rules. The two types of rules are as follows:

- Absolute—A rule with a specific start date and time, specific end date and time, both, or neither. The following items describe how the presence or absence of a start or end date and time affect whether an absolute time range rule is active:
  - Start and end date and time both specified—The time range rule is active when the current time is later than the start date and time and earlier than the end date and time.
  - Start date and time specified with no end date and time—The time range rule is active when the current time is later than the start date and time.
  - No start date and time with end date and time specified—The time range rule is active when the current time is earlier than the end date and time.

## ***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).***

- No start or end date and time specified—The time range rule is always active.

For example, you could prepare your network to allow access to a new subnet by specifying a time range that allows access beginning at midnight of the day that you plan to place the subnet online. You can use that time range in ACL rules that apply to the subnet. After the start time and date have passed, the device automatically begins applying the rules that use this time range when it applies the ACLs that contain the rules.

- Periodic—A rule that is active one or more times per week. For example, you could use a periodic time range to allow access to a lab subnet only during work hours on a weekdays. The device automatically applies ACL rules that use this time range only when the range is active and when it applies the ACLs that contain the rules.

**Note**

---

The order of rules in a time range does not affect how a device evaluates whether a time range is active.

---

Time ranges also allow you to include remarks, which you can use to insert comments into a time range. Remarks have a maximum length of 100 alphanumeric characters.

The device determines whether a time range is active as follows:

- The time range contains one or more absolute rules—The time range is active if the current time is within one or more absolute rules.
- The time range contains one or more periodic rules—The time range is active if the current time is within one or more periodic rules.
- The time range contains both absolute and periodic rules—The time range is active if the current time is within one or more absolute rules and within one or more periodic rules.

When a time range contains both absolute and periodic rules, the periodic rules can only be active when at least one absolute rule is active.

## Statistics

The device can maintain global statistics for each rule that you configure in IPv4 and MAC ACLs. If an ACL is applied to multiple interfaces, the maintained rule statistics are the sum of packet matches (hits) on all the interfaces on which that ACL is applied.

**Note**

- 
- The device does not support interface-level ACL statistics.
  - ACL statistics are not supported if the DHCP snooping feature is enabled.
- 

For each ACL that you configure, you can specify whether the device maintains statistics for that ACL, which allows you to turn ACL statistics on or off as needed to monitor traffic filtered by an ACL or to help troubleshoot the configuration of an ACL.

The device does not maintain statistics for implicit rules in an ACL. For example, the device does not maintain a count of packets that match the implicit **deny ip any any** rule at the end of all IPv4 ACLs. If you want to maintain statistics for implicit rules, you must explicitly configure the ACL with rules that are identical to the implicit rules. For more information, see the [“Implicit Rules” section on page 7-4](#).

For information about displaying IP ACL statistics, see the [“Displaying IP ACL Statistics” section on page 7-13](#). For information about displaying MAC ACL statistics, see the [“Displaying MAC ACL Statistics” section on page 8-5](#).

**[Send document comments to nexus7k-docfeedback@cisco.com.](mailto:nexus7k-docfeedback@cisco.com)**

## Virtualization Support

The following information applies to IP and MAC ACLs used in Virtual Device Contexts (VDCs):

- ACLs are unique per VDC. You cannot use an ACL that you created in one VDC in a different VDC.
- Because ACLs are not shared by VDCs, you can reuse ACL names in different VDCs.
- The device does not limit ACLs or rules on a per-VDC basis.

## Licensing Requirements for IP ACLs

The following table shows the licensing requirements for this feature:

Product	License Requirement
DCNM	IP ACLs require no license. Any feature not included in a license package is bundled with the Cisco DCNM and is provided at no charge to you. For a complete explanation of the DCNM licensing scheme, see the <i>Cisco DCNM Licensing Guide</i> .
NX-OS	IP ACLs require 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 <i>Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 4.0</i> .

## Prerequisites for IP ACLs

IP ACLs have the following prerequisites:

- You must be familiar with IP addressing and protocols to configure IP ACLs.
- You must be familiar with the interface types that you want to configure with ACLs.

## Guidelines and Limitations

IP ACLs have the following configuration guidelines and limitations:

- In most cases, ACL processing for IP packets are processed on the I/O modules. In some circumstances, processing occurs on the supervisor module, which is slower than the processing that occurs on I/O modules. Packets are processed on the supervisor module in the following circumstances:
  - Management interface traffic is always processed on the supervisor module.
  - IP packets exiting a Layer 3 interface that has an egress ACL with a large number of rules may be sent to the supervisor module.

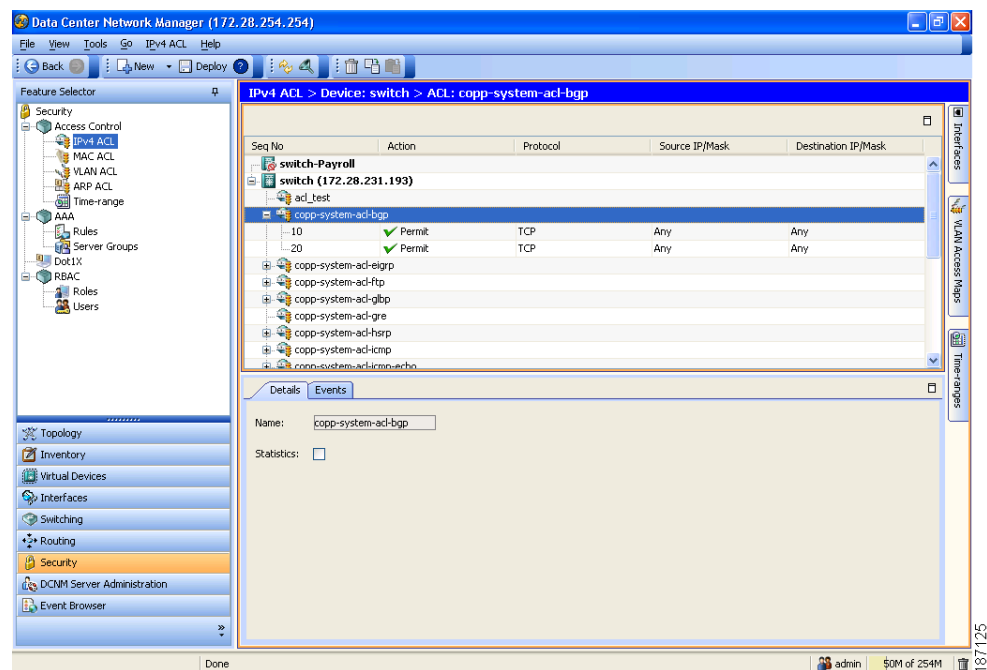
***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).***

- When you apply an ACL that uses time ranges, the device updates the ACL entries on the affected I/O modules whenever a time range referenced in an ACL entry starts or ends. Updates that are initiated by time ranges occur on a best-effort priority. If the device is especially busy when a time range causes an update, the device may delay the update by up to a few seconds.
- To apply an IP ACL to a VLAN interface, you must have enabled VLAN interfaces globally. For more information about VLAN interfaces, see the *Cisco DCNM Interfaces Configuration Guide, Release 4.0*.
- ACL statistics are not supported if the DHCP snooping feature is enabled.

## Configuring IP ACLs

Figure 7-3 shows the IPv4 ACL content pane.

**Figure 7-3 IPv4 ACL Content Pane**



This section includes the following topics:

- [Creating an IP ACL, page 7-10](#)
- [Changing an IP ACL, page 7-10](#)
- [Removing an IP ACL, page 7-11](#)
- [Applying an IP ACL to a Physical Port, page 7-11](#)
- [Applying an IP ACL to a Port Channel, page 7-12](#)
- [Applying an IP ACL as a VACL, page 7-13](#)

*Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).*

## Creating an IP ACL

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

### DETAILED STEPS

To create an IP ACL on the device, follow these steps:

- 
- Step 1** From the Feature Selector pane, choose **Security > Access Control > IPv4 ACL**.  
The available devices appear in the Summary pane.
  - Step 2** From the Summary pane, double-click the device to which you want to add an ACL.
  - Step 3** From the menu bar, choose **File > New > IPv4 ACL**.  
A new row appears in the Summary pane. The Details tab appears in the Details pane.
  - Step 4** From the Details tab, in the Name field, type a name for the ACL.
  - Step 5** (Optional) If you want the device to maintain global statistics for rules in this MAC ACL, check **Statistics**.
  - Step 6** For each rule that you want to add to the ACL, from the menu bar, choose **File > New** and choose the type of rule. From the Details tab, configure fields as needed.
  - Step 7** From the menu bar, choose **File > Deploy** to apply your changes to the device.
- 

## Changing an IP ACL

You can change, reorder, add, and remove rules in an existing IPv4 ACL.

### DETAILED STEPS

To change an IP ACL, follow these steps:

- 
- Step 1** From the Feature Selector pane, choose **Security > Access Control > IPv4 ACL**.  
The available devices appear in the Summary pane.
  - Step 2** From the Summary pane, double-click the device that has the ACL that you want to change and then double-click the ACL.  
The ACLs on the device and the rules of the ACL that you double-clicked appear in the Summary pane.
  - Step 3** (Optional) If you change whether the device maintains global statistics for rules in this IP ACL, click the ACL in the Summary pane. On the Details tab, check or uncheck **Statistics** as needed.
  - Step 4** (Optional) If you want to change the details of a rule, click the rule in the Summary pane. From the Details tab, configure fields as needed.
  - Step 5** (Optional) If you want to add a rule, click the ACL in the Summary pane and then from the menu bar, choose **File > New** and choose the type of rule. On the Details tab, configure fields as needed.
  - Step 6** (Optional) If you want to remove a rule, click the rule and then from the menu bar, choose **IPv4 ACL > Delete**.

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).***

**Step 7** (Optional) If you want to move a rule to a different position in the ACL, click the rule in the Summary pane and then from the menu bar, choose one of the following, as applicable:

- **IPv4 ACL > Move Up**
- **IPv4 ACL > Move Down**

The rule moves up or down, as you chose. The sequence number of the rules adjust accordingly.

**Step 8** From the menu bar, choose **File > Deploy** to apply your changes to the device.

---

## Removing an IP ACL

You can remove an IP ACL from the device.

### BEFORE YOU BEGIN

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

### DETAILED STEPS

To remove an IP ACL from the device, follow these steps:

- 
- Step 1** From the Feature Selector pane, choose **Security > Access Control > IPv4 ACL**.  
Available devices appear in the Summary pane.
- Step 2** From the Summary pane, double-click the device from which you want to remove an ACL.  
The ACLs currently on the device appear in the Summary pane.
- Step 3** Click the ACL that you want to remove.
- Step 4** From the menu bar, choose **IPv4 ACL > Delete**.  
The ACL disappears from the Summary pane.
- Step 5** From the menu bar, choose **File > Deploy** to apply your changes to the device.
- 

## Applying an IP ACL to a Physical Port

You can apply an IPv4 ACL to a physical Ethernet port when the port mode is set to one of the following:

- Access
- PVLAN Host
- PVLAN Promiscuous
- Routed

You cannot apply an IPv4 ACL to a port when the port mode is set to Trunk.

DCNM allows you to apply IP ACLs directionally; that is, you can specify separate ACLs for incoming traffic and outgoing traffic on a physical Ethernet port.

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).***

## BEFORE YOU BEGIN

Ensure that the ACL that 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 [“Creating an IP ACL” section on page 7-10](#) or the [“Changing an IP ACL” section on page 7-10](#).

## DETAILED STEPS

To apply an IP ACL to a physical Ethernet port, follow these steps:

- 
- Step 1** From the Feature Selector pane, choose **Interfaces > Physical > Ethernet**.  
Available devices appear in the Summary pane.
- Step 2** From the Summary pane, double-click the applicable device and then double-click the slot that contain the port.  
The ports in the slot that you double-clicked appear in the Summary pane.
- Step 3** Click the port to which you want to apply an IP ACL.  
Settings for the port that you clicked appear in the Details pane.
- Step 4** From the Details pane, click the **Details** tab and expand the **Advanced Settings** section, if necessary.  
The following drop-down lists appear in the Advanced Settings section:
- Incoming Ipv4 Traffic
  - Outgoing Ipv4 Traffic
- Step 5** For each ACL type and traffic direction that you want to apply an ACL, from the applicable drop-down list, choose the ACL that you want to apply.
- Step 6** From the menu bar, choose **File > Deploy** to apply your changes to the device.
- 

## Applying an IP ACL to a Port Channel

You can apply IPv4 ACLs to an Ethernet port channel.

DCNM allows you to apply IP ACLs directionally; you can specify separate ACLs for incoming traffic and outgoing traffic on an Ethernet port channel.

## 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 [“Creating an IP ACL” section on page 7-10](#) or the [“Changing an IP ACL” section on page 7-10](#).

## DETAILED STEPS

To apply an IP ACL to a Ethernet port channel, follow these steps:

- 
- Step 1** From the Feature Selector pane, choose **Ports > Logical > Port Channel**.  
Available devices appear in the Summary pane.
- Step 2** From the Summary pane, double-click the applicable device.

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).***

Port channels on the device that you double-clicked appear in the Summary pane.

**Step 3** Click the port channel to which you want to apply an IP ACL.

Settings about the port channel appear in the Details pane.

**Step 4** From the Details pane, click the **Port Channel Advanced Settings** tab and expand the **Advanced Settings** section, if necessary.

In the Advanced Settings section, the IPv4 ACL area contains an Incoming Traffic drop-down list and an Outgoing Traffic drop-down list.

**Step 5** For each ACL type and traffic direction that you want to apply an ACL, from the applicable drop-down list, choose the ACL that you want to apply.

**Step 6** From the menu bar, choose **File > Deploy** to apply your changes to the device.

---

## Applying an IP ACL as a VACL

You can apply an IP ACL as a VACL. For information about how to create a VACL using an IPv4ACL, see the [“Creating or Changing a VACL”](#) section on page 9-3.

## Displaying IP ACL Statistics

The following window appears in the Statistics tab:

- Access Rule Statistics Chart—Information about the number of packets that match the selected IP ACL rule.

See the *Cisco DCNM Fundamentals Configuration Guide, Release 4.0* for more information on collecting statistics for this feature.

## Field Descriptions for IPv4 ACLs

This section includes the following topics:

- [IPv4 ACL: Details Tab, page 7-14](#)
- [IPv4 Access Rule: Details Tab, page 7-14](#)
- [IPv4 Access Rule: Details: Source and Destination Section, page 7-14](#)
- [IPv4 Access Rule: Details: Protocol and Others Section, page 7-15](#)
- [IPv4 Access Rule: Details: Advanced Section, page 7-17](#)
- [IPv4 ACL Remark: Remark Details Tab, page 7-18](#)

[Send document comments to nexus7k-docfeedback@cisco.com.](mailto:nexus7k-docfeedback@cisco.com)

## IPv4 ACL: Details Tab

**Table 7-2** IPv4 ACL: Details Tab

Field	Description
Name	Name of the IPv4 ACL. Names can be a maximum of 64 alphanumeric characters but must begin with an alphabetic character. No name is assigned by default.
Statistics	Whether the device logs statistics about traffic filtered by the ACL. This check box is unchecked by default.

## IPv4 Access Rule: Details Tab

**Table 7-3** IPv4 Access Rule: Details Tab

Field	Description
Sequence Number	<i>Display only.</i> Sequence number assigned to the rule.
Action	Action taken by the device when it determines that the rule applies to the packet. Valid values are as follows: <ul style="list-style-type: none"> <li>Deny—Stops processing the packet and drop it. This is the default value.</li> <li>Permit—Continues processing the packet.</li> </ul>

## IPv4 Access Rule: Details: Source and Destination Section

**Table 7-4** IPv4 Access Rule: Details: Source and Destination Section

Field	Description
Source	Type of source. Valid values are as follows: <ul style="list-style-type: none"> <li>Any—The rule matches packets from any IPv4 source. This is the default value. When you choose Any, the IP Address and Wildcard Mask fields below this list are unavailable because you do not need to specify either of them.</li> <li>Host—The rule matches packets from a specific IPv4 address. When you choose Host, the IP Address field below this list is available but the Wildcard Mask field remains unavailable.</li> <li>Network—The rule matches packets from an IPv4 network. When you choose Network, the IP Address and Wildcard Mask fields below this list are both available.</li> </ul>
IP Address (Source)	IPv4 address of a host or a network. Valid addresses are in dotted decimal format. This field is available when you choose Host or Network from the Source drop-down list. This field is unavailable by default.

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).***

**Table 7-4 IPv4 Access Rule: Details: Source and Destination Section (continued)**

Field	Description
Wildcard Mask (Source)	Wildcard mask of an IPv4 network. Valid masks are in dotted decimal format. For example, if you specified 192.168.0.0 in the IP Address field, you would enter 0.0.255.255 in this field. This field is available when you choose Network from the Source drop-down list. This field is unavailable by default.
Destination	Type of destination. Valid values are as follows: <ul style="list-style-type: none"> <li>Any—The rule matches packets sent to any IPv4 source. This is the default value. When you choose Any, the IP Address and Wildcard Mask fields below this list are unavailable because you do not need to specify either of them.</li> <li>Host—The rule matches packets sent to a specific IPv4 address. When you choose Host, the IP Address field below this list is available but the Wildcard Mask field remains unavailable.</li> <li>Network—The rule matches packets sent to an IPv4 network. When you choose Network, the IP Address and Wildcard Mask fields below this list are both available.</li> </ul>
IP Address (Destination)	IPv4 address of a host or a network. Valid addresses are in dotted decimal format. This field is available when you choose Host or Network from the Destination drop-down list. This field is unavailable by default.
Wildcard Mask (Destination)	Wildcard mask of an IPv4 network. Valid masks are in dotted decimal format. For example, if you specified 192.168.0.0 in the IP Address field, you would enter 0.0.255.255 in this field. This field is available when you choose Network from the Destination drop-down list. This field is unavailable by default.

## IPv4 Access Rule: Details: Protocol and Others Section

**Table 7-5 IPv4 Access Rule: Details: Protocol and Others Section**

Field	Description
<b>All Access Rules</b>	
Protocol	<i>Display only.</i> Protocol of the access rule. Possible values are as follows: <ul style="list-style-type: none"> <li>IP</li> <li>TCP</li> <li>UDP</li> <li>ICMP</li> <li>IGMP</li> </ul>
Time range	Named time range that applies to the access rule. If you want the rule to be always in effect, do not specify a time range. This field is blank by default.
Log this entry	Whether the device logs statistics about traffic to which the access rule applies. This check box is unchecked by default.

**Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).**

**Table 7-5 IPv4 Access Rule: Details: Protocol and Others Section (continued)**

Field	Description
<b>IP Access Rule</b>	
IP Protocol	Type of traffic that the access rule applies to. The default value is Ip, which applies to all IP protocols. To specify a well-known protocol, choose the protocol name. The list is ordered by the protocol number. For the IANA list of assigned internet protocol numbers, see <a href="http://www.iana.org/assignments/protocol-numbers">http://www.iana.org/assignments/protocol-numbers</a> .
<b>TCP and UDP Access Rules</b>	
Source Port	<p>Source port or range of source ports to which the access rule applies. By default, no source port is assigned.</p> <p>The left list specifies the operator that the device uses when comparing the source port of packets to the port or ports specified in the access rule.</p> <p>The right field is either a drop-down list or a pair of text fields. When the operator is not Range, the drop-down list allows you to specify a well-known port by name.</p> <p>When the operator is Range, the text fields allow you to enter the beginning and ending port numbers of the range. Valid port numbers in both fields are from 0 to 65535.</p> <p><b>Tip</b> To specify a single port by number, choose Range from the operator drop-down list and enter the port number in both source port fields.</p>
Destination	<p>Destination port or range of destination ports to which the access rule applies. By default, no source port is assigned.</p> <p>The left list specifies the operator that the device uses when comparing the destination port of packets to the port or ports specified in the access rule.</p> <p>The right field is either a drop-down list or a pair of text fields. When the operator is not Range, the drop-down list allows you to specify a well-known port by name.</p> <p>When the operator is Range, the text fields allow you to enter the beginning and ending port numbers of the range. Valid port numbers in both fields are from 0 to 65535.</p> <p><b>Tip</b> To specify a single port by number, choose Range from the operator drop-down list and enter the port number in both source port fields.</p>
<b>ICMP Access Rule</b>	
ICMP Message	Rule filters based on the ICMP message that you choose in the drop-down list. By default, the radio button is selected and the list is blank.
ICMP Type	Rule filters based on the values that you specify in the drop-down list and ICMP Code field. By default, the radio button is not selected and the list is unavailable.
ICMP Code	ICMP message code that the rule uses to filter ICMP traffic. Valid input for this field varies depending upon the ICMP Type drop-down list. By default, the list is unavailable.

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).***

**Table 7-5** IPv4 Access Rule: Details: Protocol and Others Section (continued)

Field	Description
<b>IGMP Access Rule</b>	
IGMP Message	Rule filters based on the IGMP message that you choose in the IGMP Message drop-down list. The radio button is selected by default. The default value for the list is 0 (zero).
IGMP Type	Rule filters based on the IGMP message type. By default, the radio button is not selected and the list is unavailable.

## IPv4 Access Rule: Details: Advanced Section

**Table 7-6** IPv4 Access Rule: Details: Advanced Section

Field	Description
<b>All Access Rules</b>	
DSCP	Differentiated services value of the DSCP header field in IP packets. The rule applies only to packets with a matching value. No value is selected by default.
Precedence	IP Precedence field value. The rule applies only to packets with a matching value. No value is selected by default.
Fragments	Rule that can only match packets that are noninitial fragments. This check box is unchecked by default.
<b>TCP Access Rules</b>	
Established	Rule that can only match packets that belong to an established TCP connection. The device considers TCP packets with the ACK or RST bits set to belong to an established connection. This check box is unchecked by default.
Fin	Rule that can only match TCP packets that have the FIN control bit flag set. This check box is unchecked by default.
Psh	Rule that can only match TCP packets that have the PSH control bit flag set. This check box is unchecked by default.
Rst	Rule that can only match TCP packets that have the RST control bit flag set. This check box is unchecked by default.
Syn	Rule that can only match TCP packets that have the SYN control bit flag set. This check box is unchecked by default.
Urg	Rule that can only match TCP packets that have the URG control bit flag set. This check box is unchecked by default.
Ack	Rule that can only match TCP packets that have the ACK control bit flag set. This check box is unchecked by default.

**Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).**

## IPv4 ACL Remark: Remark Details Tab

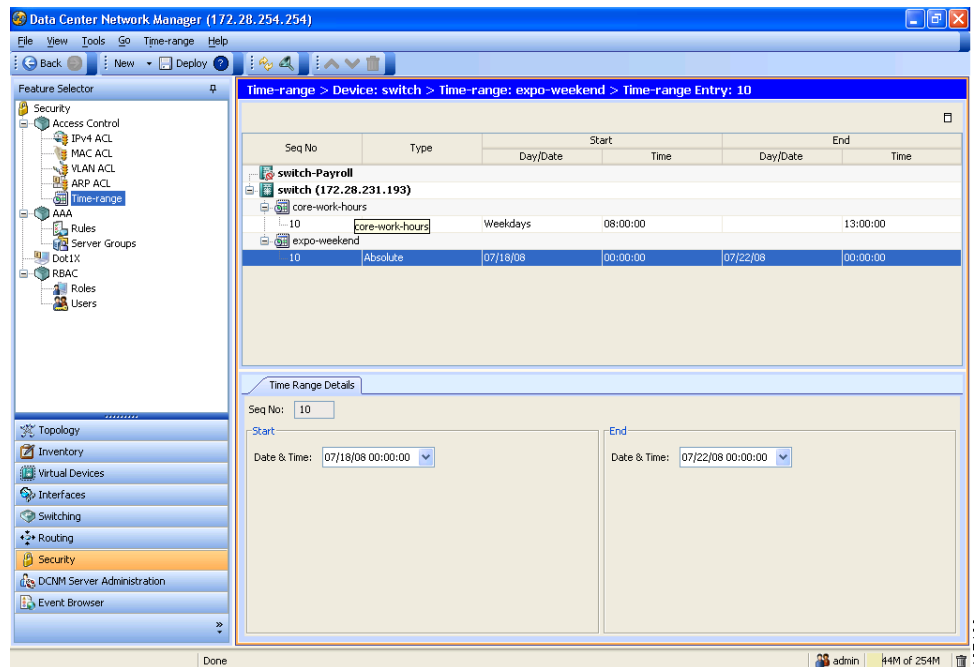
**Table 7-7** IPv4 ACL Remark: Remark Details Tab

Field	Description
Sequence Number	<i>Display only.</i> Sequence number assigned to the remark.
Remark Description	Remark text, with a maximum length of 100 alphanumeric characters. By default, this field is empty.

## Configuring Time Ranges

Figure 7-4 shows the Time-range content pane.

**Figure 7-4** Time-range Content Pane



This section includes the following topics:

- [Creating a Time Range, page 7-18](#)
- [Changing a Time Range, page 7-19](#)
- [Removing a Time Range, page 7-20](#)

## Creating a Time Range

You can create a time range on the device and add rules to it.

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).***

## DETAILED STEPS

To create a time range on the device, follow these steps:

- 
- Step 1** From the Feature Selector pane, choose **Security > Access Control > Time-range**.  
The available devices appear in the Summary pane.
- Step 2** From the Summary pane, double-click the device to which you want to add a time range.  
The time ranges present on the device, if any, appear in the Summary pane.
- Step 3** From the menu bar, choose **File > New > New Time-range**.  
A blank row appears in the Summary pane.
- Step 4** In the row, enter a name for the time range.
- Step 5** For each rule or remark that you want to add to the time range, from the menu bar, choose **File > New** and choose the type of rule or remark. On the Time Range Details tab, configure fields as needed.
- Step 6** From the menu bar, choose **File > Deploy** to apply your changes to the device.
- 

## Changing a Time Range

You can change, reorder, add, and remove rules in an existing time range.

## DETAILED STEPS

To change a time range, follow these steps:

- 
- Step 1** From the Feature Selector pane, choose **Security > Access Control > Time-range**.  
The available devices appear in the Summary pane.
- Step 2** From the Summary pane, double-click the device that has the time range that you want to change and then double-click the time range.  
Time ranges on the device and the rules of the time range that you double-clicked appear in the Summary pane.
- Step 3** (Optional) If you want to change the details of a rule, click the rule in the Summary pane. On the Time Range Details tab, configure fields as needed.
- Step 4** (Optional) If you want to move a rule to a different position in the time range, click the rule and then from the menu bar, choose one of the following, as applicable:
- **Time Range > Move Up**
  - **Time Range > Move Down**
- The rule moves up or down, as you chose. The sequence number of the rules adjust accordingly.
- Step 5** (Optional) If you want to add a rule, click the time range in the Summary pane and then from the menu bar, choose **File > New** and choose the type of rule. On the Time Range Details tab, configure fields as needed.
- Step 6** (Optional) If you want to remove a rule, click the rule in the Summary pane and then from the menu bar, choose **Time Range > Delete**.

**Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).**

**Step 7** From the menu bar, choose **File > Deploy** to apply your changes to the device.

## Removing a Time Range

You can remove a time range from the device.

### BEFORE YOU BEGIN

Ensure that you know whether the time range is used in any ACL rules. The device allows you to remove time ranges that are used in ACL rules. Removing a time range that is in use in an ACL rule does not affect the configuration of interfaces where you have applied the ACL. Instead, the device considers the ACL rule using the removed time range to be empty.

### DETAILED STEPS

To remove a time range, follow these steps:

- 
- Step 1** From the Feature Selector pane, choose **Security > Access Control > Time-range**.  
The available devices appear in the Summary pane.
- Step 2** From the Summary pane, double-click the device from which you want to remove a time range.  
Time ranges currently on the device appear in the Summary pane.
- Step 3** From the Summary pane, click the time range that you want to remove.
- Step 4** From the menu bar, choose **Time Range > Delete**.  
The time range disappears from the Summary pane.
- Step 5** From the menu bar, choose **File > Deploy** to apply your changes to the device.
- 

## Field Descriptions for Time Ranges

Table 7-8 describes the fields for time range rules and remarks.

**Table 7-8** Time Range Rule or Remark: Time Range Details Tab

Field	Description
<b>All Time Range Rules and Remarks</b>	
Seq No	<i>Display only.</i> Sequence number assigned to the rule.
<b>Remarks</b>	
Description	Remark text, with a maximum length of 100 alphanumeric characters. By default, this field is blank.
<b>Absolute Rules</b>	

**[Send document comments to nexus7k-docfeedback@cisco.com.](mailto:nexus7k-docfeedback@cisco.com)**

**Table 7-8** Time Range Rule or Remark: Time Range Details Tab (continued)

Field	Description
Date (Start)	Time and date that the absolute time range becomes active. By default, this list is blank.  You must configure either the start Date drop-down list, the end Date drop-down list, or both.
Date (End)	Time and date that the absolute time range becomes inactive. By default, this list is blank.  You must configure either the start Date drop-down list, the end Date drop-down list, or both.
<b>Periodic Rules</b>	
Days	Days of the week that the periodic rule is active. You can choose one of the following radio buttons: <ul style="list-style-type: none"> <li>• Daily—The range is active every day of the week.</li> <li>• Weekdays—The range is active Monday through Friday only.</li> <li>• Weekend—The range is active Saturday and Sunday only.</li> <li>• Specific Days—The range is active on the days specified in the Days of the week check boxes. This is the default value. The Day drop-down list (End) is available only when you choose this radio button and choose only one day in the Days of the week check boxes.</li> </ul>
Days of the week	Days of the week that the periodic rule is active. These check boxes are available only if the Specific Days radio button is selected. By default, these check boxes are unchecked.
Time (Start)	Time that the range becomes active. The time in this spin box must be before the time in the Time (End) spin box. The default value is 00:00:00.
Day	Day of the week that the time range becomes inactive. This drop-down list is available only if you select the Specific Days radio button and select only one of the check boxes under Days of the week. By default, this list is unavailable.
Time (End)	Time that the range becomes inactive. The time in this spin box must be after the time in the Time (End) spin box. The default value is 00:00:00.

## Additional References

For additional information related to implementing IP ACLs, see the following sections:

- [Related Documents, page 7-21](#)
- [Standards, page 7-22](#)

## Related Documents

Related Topic	Document Title
Concepts about VACLs	<a href="#">Information About VLAN ACLs, page 9-1</a>

## ■ Additional References

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).***

## Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—