CHAPTER 10

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 ACLs.

This chapter includes the following sections:

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 10-6.

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

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 11-1.
- Security-group ACLs (SGACLs)—The device applies SGACLs to traffic tagged by Cisco TrustSec. For more information, see Chapter 9, "Configuring Cisco TrustSec."

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 10-1 summarizes the applications for security ACLs.

Table 10-1 Security ACL Applications

Application	Supported Interfaces	Types of ACLs Supported
Port ACL	• Layer 2 interfaces • Layer 2 Ethernet port-channel interfaces When a port ACL is applied to a trunk port, the ACL filters traffic on all VLANs on the trunk port.	• IPv4 ACLs • MAC ACLs
Router ACL	• VLAN interfaces (sometimes referred to as switched virtual interfaces or SVIs) **Note** You must enable VLAN interfaces globally before you can configure a VLAN interface. For more information, see the *Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 4.0*. • Physical Layer 3 interfaces • Layer 3 Ethernet subinterfaces • Layer 3 Ethernet port-channel interfaces • Layer 3 Ethernet port-channel subinterfaces • Tunnels • Management interfaces	• IPv4 ACLs **Note** MAC ACLs are not supported on Layer 3 interfaces.
VLAN ACL	• VLANs For more information about VLAN ACLs, see Chapter 12, "Configuring VLAN ACLs."	• IPv4 ACLs • MAC ACLs

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
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. Figure 10-1 shows the order in which the device applies ACLs.

Figure 10-1 Order of ACL Application

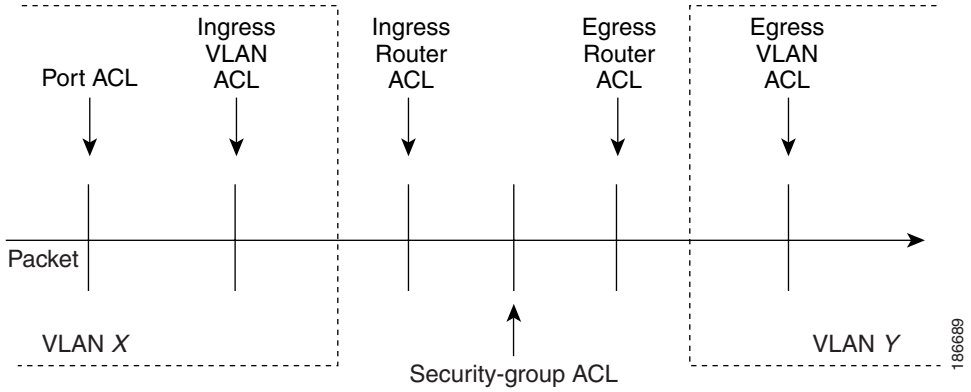
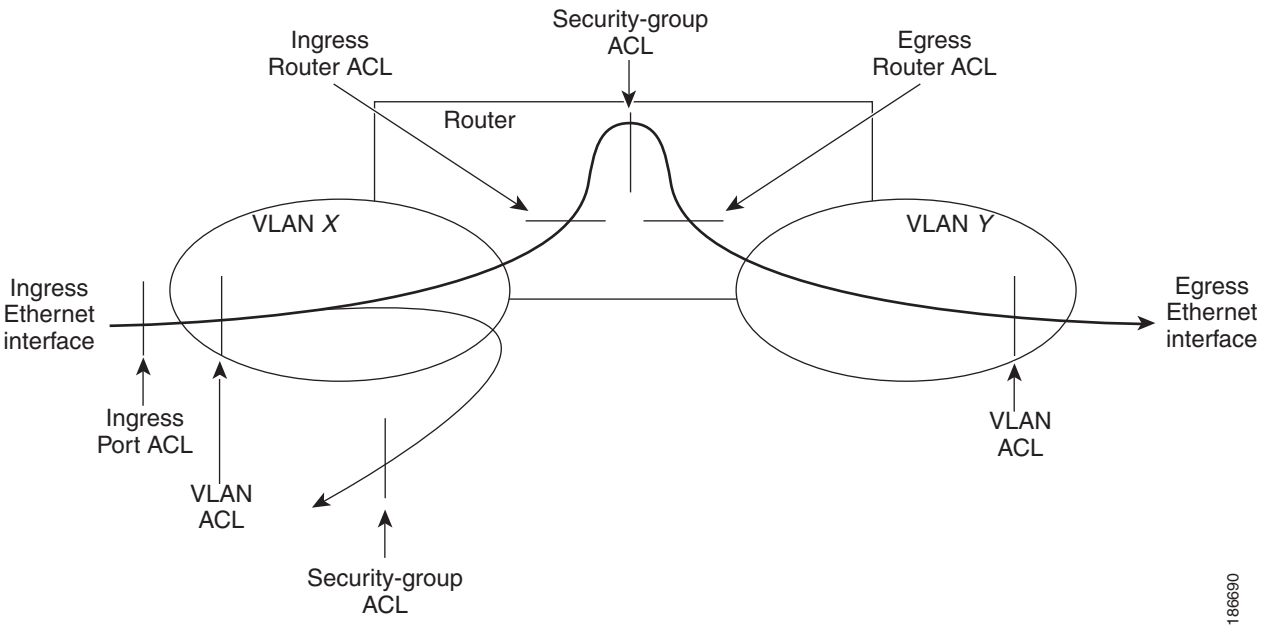


Figure 10-2 shows where the device applies ACLs, depending upon the type of ACL. The red path indicates a packet sent to a destination on a different interface than its source. The blue path indicates a packet that is bridged within its VLAN.

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.

For more information about SGACLs, see Chapter 9, "Configuring Cisco TrustSec."

Figure 10-2 ACLs and Packet Flow



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, especially if you use object groups when you configure rules. For more information, see the "Policy-Based ACLs" section on page 10-9.

You 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.

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 Nexus 7000 Series NX-OS Security Command Reference, Release 4.0*.

This section includes the following topics:

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. For information about specifying source and destination, see the applicable **permit** and **deny** commands in the *Cisco Nexus 7000 Series NX-OS Security Command Reference, Release 4.0*.

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.

For a list of the protocols that each type of ACL supports by name, see the applicable **permit** and **deny** commands in the *Cisco Nexus 7000 Series NX-OS Security Command Reference, Release 4.0*.

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.

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)

For information about all filtering options available in rules, see the applicable **permit** and **deny** commands in the *Cisco Nexus 7000 Series NX-OS Security Command Reference, Release 4.0*.

Sequence Numbers

The device supports sequence numbers for rules. Every rule that you enter receives a sequence number, either assigned by you or assigned automatically by the device. Sequence numbers simplify the following ACL tasks:

- Adding new rules between existing rules—By specifying the sequence number, you specify where in the ACL a new rule should be positioned. For example, if you need to insert a rule between rules numbered 100 and 110, you could assign a sequence number of 105 to the new rule.

- Removing a rule—Without using a sequence number, removing a rule requires that you enter the whole rule, as follows:

  ```
  switch(config-acl)# no permit tcp 10.0.0.0/8 any
  ```

  However, if the same rule had a sequence number of 101, removing the rule requires only the following command:

  ```
  switch(config-acl)# no 101
  ```

- Moving a rule—With sequence numbers, if you need to move a rule to a different position within an ACL, you can add a second instance of the rule using the sequence number that positions it correctly, and then you can remove the original instance of the rule. This action allows you to move the rule without disrupting traffic.

If you enter a rule without a sequence number, the device adds the rule to the end of the ACL and assigns a sequence number that is 10 greater than the sequence number of the preceding rule to the rule. For example, if the last rule in an ACL has a sequence number of 225 and you add a rule without a sequence number, the device assigns the sequence number 235 to the new rule.

In addition, NX-OS allows you to reassign sequence numbers to rules in an ACL. Resequencing is useful when an ACL has rules numbered contiguously, such as 100 and 101, and you need to insert one or more rules between those rules.

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.

- 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.
  - 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. NX-OS includes sequence numbers in time ranges to make editing the time range easier.

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.

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.

Using object groups when you configure IPv4 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.

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.

The following object group types apply to port, router, and VLAN ACLs:

- IPv4 address object groups—Can be used with IPv4 ACL rules to specify source or destination addresses. When you use the **permit** or **deny** command to configure a rule, the **addrgroup** keyword allows you to specify an object group for the source or destination.
- Protocol port object groups—Can be used with IPv4 TCP and UDP rules to specify source or destination ports. When you use the **permit** or **deny** command to configure a rule, the **portgroup** keyword allows you to specify an object group for the source or destination.

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 10-6.

For information about displaying IP ACL statistics, see the "Displaying and Clearing IP ACL Statistics" section on page 10-20. For information about displaying MAC ACL statistics, see the "Displaying and Clearing MAC ACL Statistics" section on page 11-8.

Session Manager Support for IP ACLs

Session Manager supports the configuration of IP and MAC ACLs. This feature allows you to verify ACL configuration and confirm that the resources required by the configuration are available prior to committing them to the running configuration. For more information about Session Manager, see the *Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 4.0*.

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
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 *Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 4.0*.

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:

- We recommend that you perform ACL configuration using the Session Manager. This feature allows you to verify ACL configuration and confirm that the resources required by the configuration are available prior to committing them to the running configuration. This is especially useful for ACLs that include more than about 1000 rules. For more information about Session Manager, see the *Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 4.0*.
- In most cases, ACL processing for IP packets occurs on the I/O modules, which use hardware that accelerates ACL processing. In some circumstances, processing occurs on the supervisor module, which can result in slower ACL processing, especially during processing that involves an ACL with a large number of rules. Management interface traffic is always processed on the supervisor module. If IP packets in any of the following categories are exiting a Layer 3 interface, they are sent to the supervisor module for processing:
  - Packets that fail the Layer 3 maximum transmission unit check and therefore require fragmenting.
  - IPv4 packets that have IP options (additional IP packet header fields following the destination address field).
  - IPv6 packets that have extended IPv6 header fields.

  Rate limiters prevent redirected packets from overwhelming the supervisor module. For more information, see Chapter 22, “Configuring Rate Limits.”
- 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 Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 4.0*.
- ACL statistics are not supported if the DHCP snooping feature is enabled.

Configuring IP ACLs

This section includes the following topics:

- Applying an IP ACL as a Router ACL, page 10-17
- Applying an IP ACL as a Port ACL, page 10-19
- Applying an IP ACL as a VACL, page 10-20

Creating an IP ACL

You can create an IPv4 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.

We recommend that you perform ACL configuration using the Session Manager. This feature allows you to verify ACL configuration and confirm that the resources required by the configuration are available prior to committing them to the running configuration. This is especially useful for ACLs that include more than about 1000 rules. For more information about Session Manager, see the *Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 4.0*.

SUMMARY STEPS

1. **configure terminal**
2. **ip access-list** *name*
3. [*sequence-number*] {**permit** | **deny**} *protocol source destination*
4. **statistics per-entry**
5. **show ip access-lists** *name*
6. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	**ip access-list** *name* **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*] {**permit** | **deny**} *protocol source 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 Nexus 7000 Series NX-OS Security Command Reference, Release 4.0*.
Step 4	**statistics per-entry** **Example:** switch(config-acl)# statistics per-entry	(Optional) Specifies that the device maintains global statistics for packets that match the rules in the ACL.
Step 5	**show ip access-lists** *name* **Example:** switch(config-acl)# show ip access-lists acl-01	(Optional) Displays the IP ACL configuration.
Step 6	**copy running-config startup-config** **Example:** switch(config-acl)# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Changing an IP ACL

You can add and remove rules in an existing IPv4 ACL. You cannot change existing rules. Instead, to change a rule, you can remove it and recreate it with the desired changes.

If you need to add more rules between existing rules than the current sequence numbering allows, you can use the **resequence** command to reassign sequence numbers. For more information, see the "Changing Sequence Numbers in an IP ACL" section on page 10-16.

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.

We recommend that you perform ACL configuration using the Session Manager. This feature allows you to verify ACL configuration and confirm that the resources required by the configuration are available prior to committing them to the running configuration. This is especially useful for ACLs that include more than about 1000 rules. For more information about Session Manager, see the *Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 4.0*.

SUMMARY STEPS

1. **configure terminal**
2. **ip 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-list** *name*
7. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

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

Step 2	**ip 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`	(Optional) 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. For more information, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference, Release 4.0*.
Step 4	**no** {*sequence-number* | {**permit** | **deny**} *protocol source destination*} **Example:** `switch(config-acl)# no 80`	(Optional) Removes the rule that you specified from the IP ACL. The **permit** and **deny** commands support many ways of identifying traffic. For more information, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference, Release 4.0*.

	Command	Purpose

Step 5	`[no] statistics per-entry`
	
	Example:
	`switch(config-acl)# statistics per-entry`
		(Optional) 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	**show ip access-lists** *name* **Example:** `switch(config-acl)# show ip access-lists acl-01`	(Optional) Displays the IP ACL configuration.
Step 7	**copy running-config startup-config** **Example:** `switch(config-acl)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Removing an IP ACL

You can remove an IP ACL from the device.

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.

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. Use the **show ip access-lists** command with the **summary** keyword to find the interfaces that an IP ACL is configured on.

SUMMARY STEPS

1. **configure terminal**
2. **no ip access-list** *name*
3. **show ip access-list** *name* **summary**
4. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	**no ip access-list** *name* **Example:** switch(config)# no ip access-list acl-01	Removes the IP ACL that you specified by name from the running configuration.
Step 3	**show ip access-list** *name* **summary** **Example:** switch(config)# show ip access-lists acl-01 summary	(Optional) Displays the IP ACL configuration. If the ACL remains applied to an interface, the command lists the interfaces.
Step 4	**copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Changing Sequence Numbers in an IP ACL

You can change all the sequence numbers assigned to the rules in an IP ACL.

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. **configure terminal**
2. **resequence ip access-list** *name starting-sequence-number increment*
3. **show ip access-lists** *name*
4. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

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

Step 2	**resequence ip access-list** *name starting-sequence-number increment* **Example:** `switch(config)# resequence access-list ip acl-01 100 10`	Assigns sequence numbers to the rules contained in the ACL, where the first rule receives 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 that you specify. The *starting-sequence-number* argument and the *increment* argument can be a whole number between 1 and 4294967295.
Step 3	**show ip access-lists** *name* **Example:** `switch(config)# show ip access-lists acl-01`	(Optional) Displays the IP ACL configuration.
Step 4	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Applying an IP ACL as a Router ACL

You can apply an IPv4 ACL to any of the following types of interfaces:

- Physical Layer 3 interfaces and subinterfaces
- Layer 3 Ethernet port-channel interfaces and subinterfaces
- VLAN interfaces
- Tunnels
- Management interfaces

ACLs applied to these interface types are considered router ACLs.

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 10-12 or the "Changing an IP ACL" section on page 10-13.

SUMMARY STEPS

1. **configure terminal**
2. **interface ethernet** *slot*/*port*[.*number*]

interface port-channel *channel-number*[**.***number*]

interface tunnel *tunnel-number*

interface vlan *vlan-ID*

interface mgmt *port*

3. **ip access-group** *access-list* {**in** | **out**}
4. **show running-config aclmgr**
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

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

Step 2	**interface ethernet** *slot/port*[**.***number*]
	
	Example:
	`switch(config)# interface ethernet 2/3`
	`switch(config-if)#`
		Enters interface configuration mode for a Layer 2 or Layer 3 physical interface. To enter configuration mode for a Layer 3 subinterface, specify the *number* argument.

	interface port-channel *channel-number*[**.***number*]
	
	Example:
	`switch(config)# interface port-channel 5`
	`switch(config-if)#`
		Enters interface configuration mode for a port channel. To enter configuration mode for a Layer 3 port-channel interface, specify the *number* argument.

	interface tunnel *tunnel-number*
	
	Example:
	`switch(config)# interface tunnel 13`
	`switch(config-if)#`
		Enters interface configuration mode for a tunnel.

	interface vlan *vlan-ID*
	
	Example:
	`switch(config)# interface vlan 11`
	`switch(config-if)#`
		Enters interface configuration mode for a VLAN interface.

	interface mgmt *port*
	
	Example:
	`switch(config)# interface mgmt 0`
	`switch(config-if)#`
		Enters interface configuration mode for a management port.

Step 3	**ip access-group** *access-list* {**in** | **out**} **Example:** `switch(config-if)# ip access-group acl-120 out`	Applies an IPv4 ACL to the Layer 3 interface for traffic flowing in the direction specified. You can apply one router ACL per direction.
Step 4	**show running-config aclmgr** **Example:** `switch(config-if)# show running-config aclmgr`	(Optional) Displays the ACL configuration.

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

Applying an IP ACL as a Port ACL

You can apply an IPv4 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.

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 10-12 or the "Changing an IP ACL" section on page 10-13.

SUMMARY STEPS

1. **configure terminal**
2. **interface ethernet** *slot/port*
   interface port-channel *channel-number*
3. **ip port access-group** *access-list* **in**
4. **show running-config aclmgr**
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

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

Step 2	**interface ethernet** *slot/port*
	
	Example:
	`switch(config)# interface ethernet 2/3`
	`switch(config-if)#`
		Enters interface configuration mode for a Layer 2 or Layer 3 physical interface.

	interface port-channel *channel-number*
	
	Example:
	`switch(config)# interface port-channel 5`
	`switch(config-if)#`
		Enters interface configuration mode for a port channel.

Step 3	**ip port access-group** *access-list* **in** **Example:** `switch(config-if)# ip port access-group acl-l2-marketing-group in`	Applies an IPv4 ACL to the interface or port channel. Only inbound filtering is supported with port ACLs. You can apply one port ACL to an interface.

	Command	Purpose
Step 4	**show running-config aclmgr** **Example:** `switch(config-if)# show running-config aclmgr`	(Optional) Displays the ACL configuration.
Step 5	**copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

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 IPv4 ACL, see the "Creating or Changing a VACL" section on page 12-3.

Verifying IP ACL Configurations

To display IP ACL configuration information, use one of the following commands:

Command	Purpose
show running-config aclmgr	Displays the ACL configuration, including IP ACL configuration and interfaces that IP ACLs are applied to.
show ip access-lists	Displays the IPv4 ACL configuration.
show running-config interface	Displays the configuration of an interface to which you have applied an ACL.

For detailed information about the fields in the output from these commands, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference, Release 4.0*.

Displaying and Clearing IP ACL Statistics

To display or clear IP ACL statistics, use one of the following commands:

Command	Purpose
show ip access-lists	Displays IPv4 ACL configuration. If the IPv4 ACL includes the **statistics per-entry** command, then the **show ip access-lists** command output includes the number of packets that have matched each rule.
clear ip access-list counters	Clears statistics for all IPv4 ACLs or for a specific IPv4 ACL.

For detailed information about these commands, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference, Release 4.0*.

Example Configuration for IP ACLs

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:

```
ip access-list acl-01
  permit ip 192.168.2.0/24 any
interface ethernet 2/1
  ip port access-group acl-01 in
```

Configuring Object Groups

You can use object groups to specify source and destination addresses and protocol ports in IPv4 ACL rules.

This section includes the following topics:

Session Manager Support for Object Groups

Session Manager supports the configuration of object groups. This feature allows you to create a configuration session and verify your object group configuration changes prior to committing them to the running configuration. For more information about Session Manager, see the *Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 4.0*.

Creating and Changing an IPv4 Address Object Group

You can create and change an IPv4 address group object.

SUMMARY STEPS

1. **configure terminal**
2. **object-group ip address** *name*
3. [*sequence-number*] {**host** *IPv4-address* | *IPv4-address network-wildcard* | *IPv4-address/prefix-len*}

   no {*sequence-number* | **host** *IPv4-address* | *IPv4-address network-wildcard* | *IPv4-address/prefix-len*}
4. **show object-group** *name*
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	**object-group ip address** *name* **Example:** switch(config)# object-group ip address ipv4-addr-group-13 switch(config-ipaddr-ogroup)#	Creates the IPv4 address object group and enters IPv4 address object-group configuration mode.
Step 3	[*sequence-number*] {**host** *IPv4-address* | *IPv4-address network-wildcard* | *IPv4-address/prefix-len*} **Example:** switch(config-ipaddr-ogroup)# host 10.99.32.6	Creates an entry in the object group. For each entry that you want to create, use the **host** command and specify a single host or omit the **host** command to specify a network of hosts.
	no [*sequence-number* | **host** *IPv4-address* | *IPv4-address network-wildcard* | *IPv4-address/prefix-len*} **Example:** switch(config-ipaddr-ogroup)# no host 10.99.32.6	Removes an entry in the object group. For each entry that you want to remove from the object group, use the **no** form of the **host** command.
Step 4	**show object-group** *name* **Example:** switch(config-ipaddr-ogroup)# show object-group ipv4-addr-group-13	(Optional) Displays the object group configuration.
Step 5	**copy running-config startup-config** **Example:** switch(config-ipaddr-ogroup)# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Creating and Changing a Protocol Port Object Group

You can create and change a protocol port object group.

SUMMARY STEPS

1. **configure terminal**
2. **object-group ip port** *name*
3. [*sequence-number*] *operator port-number* [*port-number*]

   no {*sequence-number* | *operator port-number* [*port-number*]}
4. **show object-group** *name*
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	**object-group ip port** *name* **Example:** switch(config)# object-group ip port NYC-datacenter-ports switch(config-port-ogroup)#	Creates the protocol port address object group and enters port object-group configuration mode.
Step 3	[*sequence-number*] *operator port-number* [*port-number*] **Example:** switch(config-port-ogroup)# eq 80	Creates an entry in the object group. For each entry that you want to create, use one of the following operator commands: • **eq**—Matches the port number that you specify only. • **gt**—Matches port numbers that are greater than (and not equal to) the port number that you specify. • **lt**—Matches port numbers that are less than (and not equal to) the port number that you specify. • **neq**—Matches all port numbers except for the port number that you specify. • **range**—Matches the range of port number between and including the two port numbers that you specify. **Note** The **range** command is the only operator command that requires two *port-number* arguments.
	no {*sequence-number* | *operator port-number* [*port-number*]} **Example:** switch(config-port-ogroup)# no eq 80	Removes an entry from the object group. For each entry that you want to remove, use the **no** form of the applicable operator command.
Step 4	**show object-group** *name* **Example:** switch(config-port-ogroup)# show object-group NYC-datacenter-ports	(Optional) Displays the object group configuration.
Step 5	**copy running-config startup-config** **Example:** switch(config-port-ogroup)# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Removing an Object Group

You can remove an IPv4 address object group or a protocol port object group.

SUMMARY STEPS

1. **configure terminal**
2. **no object-group** {**ip address** | **ip port**} *name*
3. **show object-group**
4. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

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

Step 2	**no object-group** {**ip address** | **ip port**} *name* **Example:** `switch(config)# no object-group ip address ipv4-addr-group-A7`	Removes the object group that you specified.
Step 3	**show object-group** **Example:** `switch(config)# show object-group`	(Optional) Displays all object groups. The removed object group should not appear.
Step 4	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Verifying Object-Group Configurations

To display object-group configuration information, use one of the following commands:

Command	Purpose
show object-group	Displays the object-group configuration
show running-config aclmgr	Displays ACL configuration, including object groups.

For detailed information about the fields in the output from these commands, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference, Release 4.0*.

Configuring Time Ranges

This section includes the following topics:

Session Manager Support for Time Ranges

Session Manager supports the configuration of time ranges. This feature allows you to create a configuration session and verify your time-range configuration changes prior to committing them to the running configuration. For more information about Session Manager, see the *Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 4.0*.

Creating a Time Range

You can create a time range 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. **configure terminal**
2. **time-range** *name*
3. [*sequence-number*] **periodic** *weekday time* **to** [*weekday*] *time*
   [*sequence-number*] **periodic** [*list-of-weekdays*] *time* **to** *time*
   [*sequence-number*] **absolute start** *time date* [**end** *time date*]
   [*sequence-number*] **absolute** [**start** *time date*] **end** *time date*
4. **show time-range** *name*
5. **copy running-config startup-config**

DETAILED STEPS

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

	Command	Purpose

Step 2	**time-range** *name*
	
	Example:
	`switch(config)# time-range workday-daytime`
	`switch(config-time-range)#`
		Creates the time range and enters time-range configuration mode.

Step 3	[*sequence-number*] **periodic** *weekday time* **to** [*weekday*] *time* **Example:** `switch(config-time-range)# periodic monday 00:00:00 to friday 23:59:59`	Creates a periodic rule that is in effect for one or more contiguous days between and including the specified start and end days and times.
	[*sequence-number*] **periodic** *list-of-weekdays time* **to** *time* **Example:** `switch(config-time-range)# periodic weekdays 06:00:00 to 20:00:00`	Creates a periodic rule that is in effect on the days specified by the *list-of-weekdays* argument between and including the specified start and end times. The following keywords are also valid values for the *list-of-weekdays* argument: • **daily**—All days of the week. • **weekdays**—Monday through Friday. • **weekend**—Saturday through Sunday.
	[*sequence-number*] **absolute start** *time date* [**end** *time date*] **Example:** `switch(config-time-range)# absolute start 1:00 15 march 2008`	Creates an absolute rule that is in effect beginning at the time and date specified after the **start** keyword. If you omit the **end** keyword, the rule is always in effect after the start time and date have passed.
	[*sequence-number*] **absolute** [start *time date*] **end** *time date* **Example:** `switch(config-time-range)# absolute end 23:59:59 31 december 2008`	Creates an absolute rule that is in effect until the time and date specified after the **end** keyword. If you omit the **start** keyword, the rule is always in effect until the end time and date have passed.
Step 4	**show time-range** *name* **Example:** `switch(config-time-range)# show time-range workday-daytime`	(Optional) Displays the time-range configuration.
Step 5	**copy running-config startup-config** **Example:** `switch(config-time-range)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Changing a Time Range

You can add and remove rules in an existing time range. You cannot change existing rules. Instead, to change a rule, you can remove it and recreate it with the desired changes.

If you need to add more rules between existing rules than the current sequence numbering allows, you can use the **resequence** command to reassign sequence numbers. For more information, see the "Changing Sequence Numbers in a Time Range" section on page 10-29.

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. **configure terminal**
2. **time-range** *name*
3. [*sequence-number*] **periodic** *weekday time* **to** [*weekday*] *time*

   [*sequence-number*] **periodic** [*list-of-weekdays*] *time* **to** *time*

   [*sequence-number*] **absolute start** *time date* [**end** *time date*]

   [*sequence-number*] **absolute** [**start** *time date*] **end** *time date*

   no {*sequence-number* | **periodic** *arguments . . .* | **absolute** *arguments . . .*}
4. **show time-range** *name*
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	**time-range** *name* **Example:** switch(config)# time-range workday-daytime switch(config-time-range)#	Enters time-range configuration mode for the specified time range.
Step 3	[*sequence-number*] **periodic** *weekday time* **to** [*weekday*] *time* **Example:** switch(config-time-range)# periodic monday 00:00:00 to friday 23:59:59	Creates a periodic rule that is in effect for one or more contiguous days between and including the specified start and end days and times.
	[*sequence-number*] **periodic** *list-of-weekdays time* **to** *time* **Example:** switch(config-time-range)# 100 periodic weekdays 05:00:00 to 22:00:00	Creates a periodic rule that is in effect on the days specified by the *list-of-weekdays* argument between and including the specified start and end times. The following keywords are also valid values for the *list-of-weekdays* argument: • **daily**—All days of the week. • **weekdays**—Monday through Friday. • **weekend**—Saturday through Sunday.
	[*sequence-number*] **absolute start** *time date* [**end** *time date*] **Example:** switch(config-time-range)# absolute start 1:00 15 march 2008	Creates an absolute rule that is in effect beginning at the time and date specified after the **start** keyword. If you omit the **end** keyword, the rule is always in effect after the start time and date have passed.
	[*sequence-number*] **absolute** [**start** *time date*] **end** *time date* **Example:** switch(config-time-range)# absolute end 23:59:59 31 december 2008	Creates an absolute rule that is in effect until the time and date specified after the **end** keyword. If you omit the **start** keyword, the rule is always in effect until the end time and date have passed.
	no {*sequence-number* | **periodic** *arguments . . .* | **absolute** *arguments. . .*} **Example:** switch(config-time-range)# no 80	Removes the specified rule from the time range.
Step 4	**show time-range** *name* **Example:** switch(config-time-range)# show time-range workday-daytime	(Optional) Displays the time-range configuration.
Step 5	**copy running-config startup-config** **Example:** switch(config-time-range)# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Removing a Time Range

You can remove a time range from the device.

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.

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.

SUMMARY STEPS

1. **configure terminal**
2. **no time-range** *name*
3. **show time-range**
4. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

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

Step 2	**no time-range** *name* **Example:** `switch(config)# no time-range daily-workhours`	Removes the time range that you specified by name.
Step 3	**show time-range** **Example:** `switch(config-time-range)# show time-range`	(Optional) Displays configuration for all time ranges. The removed time range should not appear.
Step 4	**copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Changing Sequence Numbers in a Time Range

You can change all the sequence numbers assigned to rules in a time range.

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. **configure terminal**
2. **resequence time-range** *name starting-sequence-number increment*
3. **show time-range** *name*
4. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

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

Step 2	**resequence time-range** *name starting-sequence-number increment*
	
	Example:
	`switch(config)# resequence time-range daily-workhours 100 10`
	`switch(config)#`
		Assigns sequence numbers to the rules contained in the time range, where the first rule receives 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 that you specify.

Step 3	**show time-range** *name* **Example:** `switch(config)# show time-range daily-workhours`	(Optional) Displays the time-range configuration.
Step 4	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Verifying Time-Range Configurations

To display time-range configuration information, use one of the following commands:

Command	Purpose
show time-range	Displays the time-range configuration
show running-config aclmgr	Displays ACL configuration, including all time ranges.

For detailed information about the fields in the output from these commands, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference, Release 4.0*.

Default Settings

Table 10-2 lists the default settings for IP ACL parameters.

Table 10-2 Default IP ACL Parameters

Parameters	Default
IP ACLs	No IP ACLs exist by default
ACL rules	Implicit rules apply to all ACLs (see the "Implicit Rules" section on page 10-6)
Object groups	No object groups exist by default
Time ranges	No time ranges exist by default

Additional References

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

- Related Documents, page 10-31
- Standards, page 10-31

Related Documents

Related Topic	Document Title
Concepts about VACLs	*Information About VLAN ACLs, page 12-1*
IP ACL commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco Nexus 7000 Series NX-OS Security Command Reference, Release 4.0*
Object group commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco Nexus 7000 Series NX-OS Security Command Reference, Release 4.0*
Time range commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco Nexus 7000 Series NX-OS Security Command Reference, Release 4.0*

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.	—

Feature History for IP ACLs

Table 10-3 lists the release history for this feature.

Table 10-3 Feature History for IP ACLs

Feature Name	Releases	Feature Information
Statistics	4.0(3)	The name of the **statistics** command was changed to **statistics per-entry**.
IP ACLs	4.0(1)	This feature was introduced.