Configuring IP ACLs

This chapter describes how to configure IP access control lists (ACLs) on the Cisco 1000 Series Connected Grid Routers (hereafter referred to as the Cisco CG-OS router).

Unless otherwise specified, the term IP ACL refers to IPv4 and IPv6 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 Cisco CG-OS router 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 Cisco CG-OS router applies the applicable default rule. The Cisco CG-OS router continues processing packets that are permitted and drops packets that are denied. For more information, see Implicit Rules, page 9-3.

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 Cisco CG-OS router supports the following types of ACLs for security traffic filtering:

- IPv4 ACLs—The Cisco CG-OS router applies IPv4 ACLs only to IPv4 traffic.
- IPv6 ACLs— The Cisco CG-OS router applies IPv6 ACLs only to IPv6 traffic.

IP ACLs supports the following Router ACL application, which filters Layer 3 traffic.

Table 9-1 summarizes the applications for security ACLs.

Table 9-1 Security ACL Applications

Application	Supported Interfaces	Types of ACLs Supported
Router ACL	Physical Layer 3 interfaces	IPv4 ACLs
	Tunnels	IPv6 ACLs

Order of ACL Application

When the Cisco CG-OS router processes a packet, it determines the forwarding path of the packet. The path determines which ACLs that the Cisco CG-OS router applies to the traffic. The Cisco CG-OS router applies the ACLs in the following order:

1. Ingress router ACL
2. Egress router ACL

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 Cisco CG-OS router creates ACL entries from the rules in the running configuration and sends those ACL entries to the applicable interface. Depending on how you configure the ACL, there might be more ACL entries than rules, especially if you use object groups when you configure rules. For more information, see Policy-Based ACLs, page 9-7.

You can create rules in access-list configuration mode by using the **permit** or **deny** command. The Cisco CG-OS router 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:

Protocols

IPv4 and IPv6 ACLs allow you to identify traffic by protocol. For your convenience, you can specify some protocols by name. For example, in an IPv4 or IPv6 ACL, you can specify ICMP by name.

You can specify any protocol by number. In IPv4 and IPv6 ACLs, you can specify protocols by the integer that represents the Internet protocol number.

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 and IPv6 ACLs. For information about specifying source and destination, see the applicable **permit** and **deny** commands.

Implicit Rules

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

IPv4 Implicit Rules

All IPv4 ACLs include the following implicit rule:

```
deny ip any any
```

This implicit rule ensures that the Cisco CG-OS router denies unmatched IP traffic.

IPv6 Implicit Rules

All IPv6 ACLs include the following implicit rules:

```
permit icmp any any nd-na
permit icmp any any nd-ns
permit icmp any any router-advertisement
permit icmp any any router-solicitation
deny ipv6 any any
```

Unless you configure an IPv6 ACL with a rule that denies ICMPv6 neighbor discovery messages, the first four rules ensure that the Cisco CG-OS router permits neighbor discovery advertisement and solicitation messages. The fifth rule ensures that the Cisco CG-OS router denies unmatched IPv6 traffic.

Note If you explicitly configure an IPv6 ACL with a **deny ipv6 any any** rule, the implicit permit rules can never permit traffic. If you explicitly configure a **deny ipv6 any any** rule but want to permit ICMPv6 neighbor discovery messages, explicitly configure a rule for all five implicit IPv6 ACL rules.

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:
  - Authentication Header Protocol
  - Encapsulating Security Payload
  - KA9Q NOS-compatible IP-over-IP tunneling
  - Open Shortest Path First (OSPF versions 2 and 3)
  - Payload Compression 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
  - Packet length
- IPv6 ACLs support the following additional filtering options:
  - Layer 4 protocol
  - Authentication Header Protocol
  - Encapsulating Security Payload
  - Payload Compression Protocol
  - Stream Control Transmission Protocol (SCTP)
  - TCP and UDP ports
  - ICMP types and codes
  - IGMP types
  - Flow label
  - DSCP value
  - TCP packets with the ACK, FIN, PSH, RST, SYN, or URG bit set
  - Established TCP connections
  - Packet length

For information about all filtering options available in rules, see the applicable **permit** and **deny** commands in the Command Lookup Tool on Cisco.com.

Sequence Numbers

The Cisco CG-OS router supports sequence numbers for rules. Every rule that you enter receives a sequence number, either assigned by you or assigned automatically by the Cisco CG-OS router. 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:

  ```
  router(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:

  ```
  router(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.

When you enter a rule without a sequence number, the Cisco CG-OS router 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 Cisco CG-OS router assigns the sequence number 235 to the new rule.

In addition, Cisco CG-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 Cisco CG-OS router stores operator-operand couples in registers called logical operator units (LOUs). The Cisco CG-OS router supports 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 Cisco CG-OS router 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.

Logging

You can enable the Cisco CG-OS router to create an informational log message for packets that match a rule.

Note ACL logging supports ACL processing that occurs on interfaces only. For more information about ACL processing, see Guidelines and Limitations, page 9-8.

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

Time Ranges

You can use time ranges to control when an ACL rule is in effect. For example, if the Cisco CG-OS router 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 Cisco CG-OS router does not compare the traffic to that rule. The Cisco CG-OS router evaluates time ranges based on its clock.

When you apply an ACL that uses time ranges, the Cisco CG-OS router updates the affected interface whenever a time range referenced in the ACL starts or ends. Updates that are initiated by time ranges occur on a best-effort priority. When the Cisco CG-OS router is especially busy when a time range causes an update, the Cisco CG-OS router might delay the update by up to a few seconds.

IPv4 and IPv6 support time ranges. When the Cisco CG-OS router 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 Cisco CG-OS router applies the ACL to traffic.

The Cisco CG-OS router 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 Cisco CG-OS router 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 weekdays. The Cisco CG-OS router 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 Cisco CG-OS router evaluates whether a time range is active. Cisco CG-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 Cisco CG-OS router 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 Cisco CG-OS router 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.

Using object groups when you configure IPv4 or IPv6 ACLs can help reduce the complexity of updating ACLs when you need to add or remove addresses 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 Cisco CG-OS router 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 interface 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 the Cisco CG-OS router:

- 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.

- IPv6 address object groups—Can be used with IPv6 ACL rules to specify source or destination addresses. When you use the **permit** or **deny** command to configure a rule, the **addrgroup** keyword allows you to specify an object group for the source or destination.

Statistics

The Cisco CG-OS router can maintain global statistics for each rule that you configure in IPv4 and IPv6 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 Cisco CG-OS router 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 Cisco CG-OS router 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 Cisco CG-OS router does not maintain statistics for implicit rules in an ACL. For example, the Cisco CG-OS router 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, then you must explicitly configure the ACL with rules that are identical to the implicit rules. For more information, see Implicit Rules, page 9-3.

For information about displaying IP ACL statistics, see Monitoring and Clearing IP ACL Statistics, page 9-14.

Session Manager Support for IP ACLs

Session Manager supports the configuration of IP 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.

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

Cisco recommends 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.

In most cases, ACL processing for IP packets occurs on the interfaces, which use hardware that accelerates ACL processing. Management interface traffic is always processed on the main board of the Cisco CG-OS router as are IP packets (in any of the following categories) that are exiting a Layer 3 interface:

- 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.
- When you apply an ACL that uses time ranges, the Cisco CG-OS router updates the ACL entries on the affected interfaces 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. When the Cisco CG-OS router is especially busy when a time range causes an update, the Cisco CG-OS router may delay the update by up to a few seconds.

Default Settings

Table 9-2 lists the default settings for IP ACL parameters.

Table 9-2 Default IP ACL Parameters

Parameters	Default
IP ACLs	No IP ACLs exist by default.
ACL rules	Implicit rules apply to all ACLs. (See Implicit Rules, page 9-3.)
Object groups	No object groups exist by default.
Time ranges	No time ranges exist by default.

Configuring IP ACLs

This section includes the following topics:

Creating an IP ACL

You can create an IPv4 ACL or IPv6 ACL on the Cisco CG-OS router and add rules to it.

BEFORE YOU BEGIN

Cisco recommends 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.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	{**ip** | **ipv6**} **access-list** *name*	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*	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.
Step 4	**statistics per-entry**	(Optional) Specifies that the Cisco CG-OS router maintains global statistics for packets that match the rules in the ACL.
Step 5	**show ip access-lists** *name*	(Optional) Displays the IP ACL configuration.
Step 6	**copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to create an IP ACL.

```
router# configure terminal
router(config)# ip access-list acl-01
router(config-acl)# permit ip 192.168.2.0/24 any
router(config-acl)# statistics per-entry
router(config-acl)# copy running-config startup-config
```

Changing an IP ACL

You can add and remove rules in an existing IPv4 or IPv6 ACL. You cannot change existing rules. Instead, to change a rule, you can remove it and recreate it with the desired changes.

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 Changing Sequence Numbers in an IP ACL, page 9-11.

BEFORE YOU BEGIN

Cisco recommends 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.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	{**ip** | **ipv6**} **access-list** *name*	Enters IP ACL configuration mode for the ACL that you specify by name.
Step 3	[*sequence-number*] {**permit** | **deny**} *protocol source destination*	(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.
Step 4	**no** {*sequence-number* | {**permit** | **deny**} *protocol source destination*}	(Optional) Removes the rule that you specified from the IP ACL. The **permit** and **deny** commands support many ways of identifying traffic.
Step 5	[**no**] **statistics per-entry**	(Optional) Specifies that the Cisco CG-OS router maintains global statistics for packets that match the rules in the ACL. The **no** option stops the Cisco CG-OS router from maintaining global statistics for the ACL.
Step 6	**show ip access-lists** *name*	(Optional) Displays the IP ACL configuration.
Step 7	**copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to change an IP ACL.

```
router# configure terminal
router(config)# ip access-list acl-01
router(config-acl)# 100 permit ip 192.168.2.0/24 any
router(config-acl)# no 80
router(config-acl)# statistics per-entry
router(config-acl)# copy running-config startup-config
```

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

No prerequisites.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**resequence** {**ip** | **ipv6**} **access-list** *name starting-sequence-number increment*	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*	(Optional) Displays the IP ACL configuration.
Step 4	**copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to change sequence numbers in an IP ACL.

```
router# configure terminal
router(config)# resequence access-list ip acl-01 100 10
router(config)# copy running-config startup-config
```

Removing an IP ACL

You can remove an IP ACL from the Cisco CG-OS router.

BEFORE YOU BEGIN

Ensure that you know whether the ACL is applied to an interface. The Cisco CG-OS router 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 Cisco CG-OS router considers the removed ACL to be empty. Use the **show ip access-lists** command or the **show ipv6 access-lists** command with the **summary** keyword to find the interfaces that an IP ACL is configured on.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**no** {**ip** | **ipv6**} **access-list** *name*	Removes the IP ACL that you specified by name from the running configuration.

	Command	Purpose
Step 3	**show** {**ip** | **ipv6**} **access-list** *name* **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**	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to remove an ACL.

```
router# configure terminal
router(config)# no ip access-list acl-01
router(config)# copy running-config startup-config
```

Applying an IP ACL as a Router ACL

You can apply an IPv4 or IPv6 ACL to any of the following types of interfaces:

- Physical Layer 3 interfaces
- Tunnels

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 Creating an IP ACL, page 9-9 or Changing an IP ACL, page 9-10.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**interface {ethernet | cellular | wimax}** *slot*//*number*]	Enters interface configuration mode for a Layer 3 physical interface.
	interface tunnel *tunnel-number*	Enters interface configuration mode for a tunnel.
Step 3	{**ip access-group** | **ipv6 traffic-filter**} *access-list* {**in** | **out**}	Applies an IPv4 or IPv6 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**r	(Optional) Displays the ACL configuration.
Step 5	**copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to apply an IPv4 ACL to a cellular interface.

```
router# configure terminal
router(config)# interface cellular 3/1
router(config-if)# ip access-group acl-20 out
router(config-if)# copy running-config startup-config
```

Verifying 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 ipv6 access-lists	Displays the IPv6 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, refer to the Command Lookup Tool on Cisco.com.

Monitoring 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.
show ipv6 access-lists	Displays IPv6 ACL configuration. If the IPv6 ACL includes the **statistics per-entry** command, then the **show ipv6 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.
clear ipv6 access-list counters	Clears statistics for all IPv6 ACLs.

For detailed information about the fields in the output from these commands, refer to the Command Lookup Tool on Cisco.com.

Configuration Example

The following example shows how to create an IPv6 ACL named acl-120 and apply it as a router ACL to Ethernet interface 2/3, which is a Layer 3 interface:

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

Configuring Object Groups

You can use object groups to specify source and destination addresses in IPv4 ACL and IPv6 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.

Creating and Changing an IPv4 Address Object Group

You can create and change an IPv4 address group object.

BEFORE YOU BEGIN

No prerequisites.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**object-group ip address** *name*	Creates the IPv4 address object group and enters IPv4 address object-group configuration mode. *name*–Maximum of 64 characters allowed.

	Command	Purpose
Step 3	[*sequence-number*] {**host** *IPv4-address* | *IPv4-address network-wildcard* | *IPv4-address/prefix-len*}	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*}	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*	(Optional) Displays the object group configuration.
Step 5	**copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to create and change an object group:

```
router# configure terminal
router (config)# object-group ip address ipv4-addr-group-13
router(config-ipaddr-ogroup)# host 10.99.32.6
router(config-ipaddr-ogroup)# copy running-config startup-config
```

Creating and Changing an IPv6 Address Object Group

You can create and change an IPv6 address group object.

BEFORE YOU BEGIN

No prerequisites.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**object-group ipv6 address** *name*	Creates the IPv6 address object group and enters IPv6 address object-group configuration mode. *name*–Maximum of 64 characters allowed.
Step 3	[*sequence-number*] {**host** *IPv6-address* | *IPv6-address/prefix-len*}	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 specify a network of hosts.
	no [*sequence-number* | **host** *IPv6-address* | *IPv6-address/prefix-len*}	Removes an entry from 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*	(Optional) Displays the object group configuration.
Step 5	**copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to create and change an IPv6 address group object.

```
router# configure terminal
router (config)# object-group ipv6 address ipv6-addr-group-A7
router(config-ipv6addr-ogroup)# host 2001:db8:0:3ab0::1
router(config-ipv6addr-ogroup)# copy running-config startup-config
```

Removing an Object Group

You can remove an IPv4 address object group and an IPv6 address object group.

BEFORE YOU BEGIN

No prerequisites.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**no object-group** {**ip address** | **ipv6 address**} *name*	Removes the object group that you specified.
Step 3	**show object-group**	(Optional) Displays all object groups. The removed object group should not appear.
Step 4	**copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to remove an IPv6 object group.

```
router# configure terminal
router (config)# no object-group ipv6 address ipv6-addr-group-A7
router(config-ipv6addr-ogroup)# copy running-config startup-config
```

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 Command Lookup Tool on Cisco.com.

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.

Creating a Time Range

You can create a time range on the Cisco CG-OS router and add rules to it.

BEFORE YOU BEGIN

No prerequisites.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**time-range** *name*	Creates the time range and enters time-range configuration mode.

	Command	Purpose
Step 3	[*sequence-number*] **periodic** *weekday time* **to** [*weekday*] *time*	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*	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*]	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*	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*	(Optional) Displays the time-range configuration.
Step 5	**copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to create a time range on the Cisco CG-OS router and add rules to it.

```
router# configure terminal
router (config)# time-range workday-daytime
router(config-time-range)# periodic monday 00:00:00 to friday 23:59:59
router(config-time-range)# copy running-config startup-config
```

Changing a Time Range

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

Note You cannot change existing rules. Instead, to change a rule, you can remove it using the no version of the command and recreate it with the desired changes.

When 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, page 9-21.

BEFORE YOU BEGIN

No prerequisites.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**time-range** *name*	Enters time-range configuration mode for the specified time range.
Step 3	[*sequence-number*] **periodic** *weekday time* **to** [*weekday*] *time*	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*	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*]	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*	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*. . .}	Removes the specified (existing) rule from the time range.
Step 4	**show time-range** *name*	(Optional) Displays the time-range configuration.
Step 5	**copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to change a time range.

```
router# configure terminal
router (config)# time-range workday-daytime
router(config-time-range)# no periodic monday 00:00:00 to friday 23:59:59
router(config-time-range)# periodic weekdays 05:00:00 to 22:00:00
```

```
router(config-time-range)# copy running-config startup-config
```

Removing a Time Range

You can remove a time range from the Cisco CG-OS router.

BEFORE YOU BEGIN

Ensure that you know whether the time range is used in any ACL rules. The Cisco CG-OS router 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 Cisco CG-OS router considers the ACL rule using the removed time range to be empty.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**no time-range** *name*	Removes the time range that you specified by name.
Step 3	**show time-range**	(Optional) Displays configuration for all time ranges. The removed time range should not appear.
Step 4	**copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to remove a time range.

```
router# configure terminal
router (config)# time-range workday-daytime
router(config-time-range)# no periodic monday 00:00:00 to friday 23:59:59
router(config-time-range)# copy running-config startup-config
```

Changing Sequence Numbers in a Time Range

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

BEFORE YOU BEGIN

No prerequisites.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**resequence time-range** *name starting-sequence-number increment*	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*	(Optional) Displays the time-range configuration.
Step 4	**copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to change a sequence number that is assigned to a rule in a time range.

```
router# configure terminal
router(config)# resequence time-range daily-workhours 100 10
router(config)# copy running-config startup-config
```

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 Command Lookup Tool on Cisco.com.