Configure Access Control List

This chapter describes the Access Control List (ACL) and the procedures to configure ACL.

Access Control List

Table 1: Feature History

Feature Name	Release Information	Feature Description
ACL on Management Port	Cisco IOS XR Release 7.11.1	Access Control List feature enables you to permit or deny specific devices to connect to the management port and access NCS 1010 devices. This control enhances network security. Both IPv4 and IPv6 ACLs are supported on the management port. Commands added: • **ipv4-access-list** • **ipv4-access-group** • **show access-lists-ipv4** • **ipv6-access-list** • **ipv6-access-group** • **show access-lists-ipv6**

Access Control List

Access Control List (ACL) is a sequential list consisting of permit and deny statements that apply to IP addresses. ACL performs packet filtering to control the packets that move through the network. These controls allow to restrict the access of devices to the network and limit network traffic.

Access Control Entries

Access Control Entries (ACE) are entries in an ACL that describe the access rights related to a particular security identifier or user. An ACL consists of one or more access control entries (ACE) that collectively define the network traffic profile.

Types of Access Control List

ACL types have different set of verification parameters and traffic control methods.

Table 2: Types of ACL

ACL Type	Verifies	Controls traffic by
Standard ACL	only the source IP address of the packets.	comparing the IP address that is configured in the ACL with the source IP address in the packet.
Extended ACL	• source address • destination address • UDP or TCP port numbers, and • Differentiated Services Code Point (DSCP) of the packets.	comparing the attributes that are defined in the ACL with those in the incoming or outgoing packets.

Benefits of Access Control List

ACL allows you to

- filter incoming or outgoing packets on an interface
- restrict the contents of routing updates
- limit debug output that is based on an address or protocol, and
- control vty access.

Guidelines and Restrictions for Access Control List

Guidelines for Access Control List

- Create an ACL before applying it to an interface.
- Write a helpful remark before or after any statement to clarify its purpose.

- Reference an ACL using a command that accepts it after you name the ACL.
- Organize the ACL so that more specific references in a network or subnet appear before more general ones.

Restrictions for Access Control List

- You must configure an ACL name up to 64 characters.
- You must configure an ACL name to comprise only letters and numbers.
- You must configure an ACL to control traffic ingressing or egressing a device but not traffic originating at the device.

Ingress and Egress Access Control Lists

Entries within the ACL are based on the direction of the flow of traffic from the point of view of the management interface of NCS 1000. ACL is applied either on the ingress or egress interfaces. Ingress ACL controls traffic that comes from a network to the management interface. Egress ACL controls traffic that comes from the management interface to the network.

The software checks the source address of the packet against the ingress or egress ACL after receiving a packet.

Table 3: Permission and Rejection of Source Address by ACL

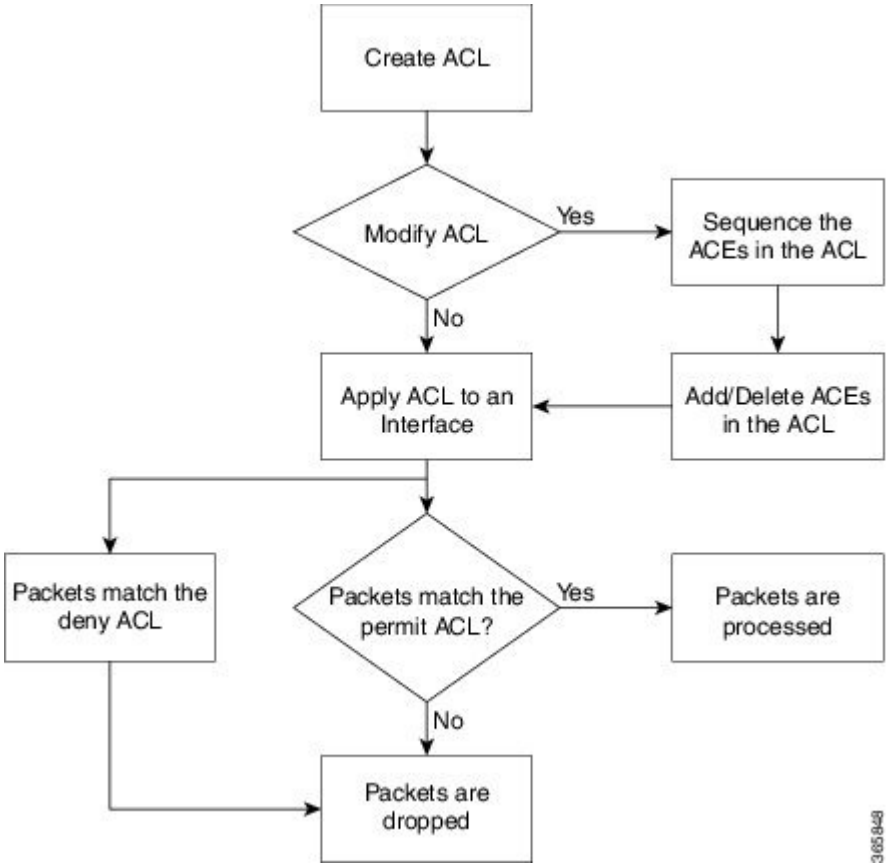
When ACL is ...	And ACL ...	Then ...
Ingress ACL	permits the source address	software continues to process the packet.
	rejects the source address	software discards the packet and returns an Internet Control Message Protocol (ICMP) host unreachable message.
Egress ACL	permits the source address	software sends the packet.
	rejects the source address	software discards the packet and returns an ICMP host unreachable message.

How an Access Control List Works

ACL Workflow

This image illustrates the workflow of an ACL.

Figure 1: ACL Workflow



Configure IPv4 Standard ACL on Management Ethernet Interface

Follow these steps to configure an IPv4 standard ACL on the management Ethernet interface.

Before you begin

Review the "Guidelines" and "Restrictions" sections of Access Control List, on page 1.

Step 1 Run the **ipv4 address** command to configure the management Ethernet interface with an IPv4 address.

Example:

```
RP/0/RP0/CPU0:ios#configure
Thu Oct 19 17:30:23.719 UTC
RP/0/RP0/CPU0:ios(config)#
RP/0/RP0/CPU0:ios(config)#interface mgmtEth 0/RP0/CPU0/0
RP/0/RP0/CPU0:ios(config-if)#ipv4 address 192.0.2.127 255.255.255.0
RP/0/RP0/CPU0:ios(config-if)#no shutdown
RP/0/RP0/CPU0:ios(config-if)#commit
Thu Oct 19 17:31:25.127 UTC
RP/0/RP0/CPU0:ios(config-if)#exit
```

Step 2 Run the **show ipv4 interface brief** command to verify whether the management Ethernet interface is up.

The entry highlighted in bold shows the status of management Ethernet interface as **Up**.

Example:

```
RP/0/RP0/CPU0:ios(config)#show ipv4 interface brief
Thu Oct 19 17:32:10.998 UTC

Interface                      IP-Address      Status          Protocol Vrf-Name
Loopback0                      192.0.2.121     Up              Up       default
GigabitEthernet0/0/0/0         192.0.2.123     Up              Up       default
GigabitEthernet0/0/0/2         192.0.2.122     Up              Up       default
MgmtEth0/RP0/CPU0/0            192.0.2.127       Up              Up       default
PTP0/RP0/CPU0/0                unassigned      Shutdown        Down     default
MgmtEth0/RP0/CPU0/1            192.0.2.124     Up              Up       default
PTP0/RP0/CPU0/1                unassigned      Shutdown        Down     default
MgmtEth0/RP0/CPU0/2            192.0.2.1       Down            Down     default
```

Step 3 Run the **ipv4 access-list** command to configure an IPv4 ACL.

Example:

```
/* Configure an IPv4 ingress ACL */
RP/0/RP0/CPU0:ios(config)# ipv4 access-list V4-ACL-INGRESS
RP/0/RP0/CPU0:ios(config-ipv4-acl)# 10 permit tcp 192.0.2.2 255.255.255.0 any
RP/0/RP0/CPU0:ios(config-ipv4-acl)# 20 deny udp any any
RP/0/RP0/CPU0:ios(config-ipv4-acl)# 30 permit ipv4 192.0.2.64 255.255.255.0 any
RP/0/RP0/CPU0:ios(config-ipv4-acl)# commit
Thu Oct 19 18:31:25.127 UTC


/* Configure an IPv4 egress ACL */
RP/0/RP0/CPU0:ios(config)# ipv4 access-list V4-ACL-EGRESS
RP/0/RP0/CPU0:ios(config-ipv4-acl)# 10 permit ipv4 203.0.113.1 255.255.255.0 192.0.2.1 0.255.255.255
RP/0/RP0/CPU0:ios(config-ipv4-acl)# 20 deny udp any any
RP/0/RP0/CPU0:ios(config-ipv4-acl)# commit
Thu Oct 19 18:31:25.127 UTC
```

Step 4 Run the **show access-lists ipv4** command to verify the ACL creation.

The entries highlighted in bold show the successful creation of ingress ACL and egresss ACL.

Example:

```
/* Verify the ingress ACL creation */
RP/0/RP0/CPU0:ios(config)# show access-lists ipv4
Thu Oct 19 18:32:25.127 UTC
ipv4 access-list V4-ACL-INGRESS
 10 permit tcp 192.0.2.2 255.255.255.0 any
 20 deny udp any any
 30 permit ipv4 192.0.2.64 255.255.255.0 any


/* Verify the egress ACL creation */
RP/0/RP0/CPU0:ios(config)# show access-lists ipv4
Thu Oct 19 18:32:25.127 UTC
ipv4 access-list V4-ACL-EGRESS
 10 permit ipv4 203.0.113.1 255.255.255.0 192.0.2.1 255.255.255.0
 20 deny ipv4 any any
```

Step 5 Run the **ipv4 access-group** command to apply the ACL to the management Ethernet interface.

Example:

```
/* Apply the ingress ACL to the mgmtEth interface */
RP/0/RP0/CPU0:ios(config)# interface mgmtEth 0/RP0/CPU0/0
RP/0/RP0/CPU0:ios(config-if)# ipv4 access-group V4-ACL-INGRESS ingress
RP/0/RP0/CPU0:ios(config-if)#commit
Thu Oct 19 18:34:25.127 UTC
RP/0/RP0/CPU0:ios(config-if)#exit


/* Apply the egress ACL to the mgmtEth interface */
RP/0/RP0/CPU0:ios(config)# interface mgmtEth 0/RP0/CPU0/0
RP/0/RP0/CPU0:ios(config-if)# ipv4 access-group V4-ACL-EGRESS egress
RP/0/RP0/CPU0:ios(config-if)# commit
Thu Jul 11 09:19:49.569 UTC
RP/0/RP0/CPU0:ios(config-if)# exit
```

Step 6 Run the **show ipv4 interface** command to verify whether the ACL has been successfully applied to the management Ethernet interface.

The entry highlighted in bold shows the ACL has been successfully applied to the management Ethernet interface.

Example:

```
/* Verify if the ingress ACL has been successfully applied to the mgmtEth interface */
RP/0/RP0/CPU0:ios#show ipv4 interface mgmtEth 0/RP0/CPU0/0
Fri Oct 20 05:07:06.383 UTC
MgmtEth0/RP0/CPU0/0 is Up, ipv4 protocol is Up
  Vrf is default (vrfid 0x60000000)
  Internet address is 192.0.2.127/16
  MTU is 1514 (1500 is available to IP)
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  common access list is not set, access list is V4-ACL-INGRESS
  Proxy ARP is disabled
  ICMP redirects are never sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  Table Id is 0xe0000000
/* Verify if the egress ACL has been successfully applied to the mgmtEth interface */

RP/0/RP0/CPU0:ios#show ipv4 interface mgmtEth 0/RP0/CPU0/0
Fri Oct 20 05:07:06.383 UTC
MgmtEth0/RP0/CPU0/0 is Up, ipv4 protocol is Up
  Vrf is default (vrfid 0x60000000)
  Internet address is 192.0.2.127/16
  MTU is 1514 (1500 is available to IP)
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is V4-ACL-EGRESS
  Inbound  common access list is not set, access list is not set
  Proxy ARP is disabled
  ICMP redirects are never sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  Table Id is 0xe0000000
```

You have successfully configured an IPv4 standard ACL on the management Ethernet interface.

Configure IPv6 Standard Access Control List on Management Ethernet Interface

Follow these steps to configure an IPv6 standard ACL on the management Ethernet interface.

Before you begin

Review the "Guidelines" and "Restrictions" sections of Access Control List, on page 1.

Step 1 Run the **ipv6 address** command to configure the management Ethernet interface with an IPv6 address.

Example:

```
RP/0/RP0/CPU0:ios#configure
Fri Oct 20 05:25:58.785 UTC
RP/0/RP0/CPU0:ios(config)#interface mgmtEth 0/RP0/CPU0/1
RP/0/RP0/CPU0:ios(config-if)#ipv6 address 2001::1/64
RP/0/RP0/CPU0:ios(config-if)#no shutdown
RP/0/RP0/CPU0:ios(config-if)#commit
Fri Oct 20 05:26:13.669 UTC
RP/0/RP0/CPU0:ios(config-if)#exit
```

Step 2 Run the **show ipv6 interface** command to verify whether the management Ethernet interface is up.

The entry highlighted in bold shows the status of management Ethernet interface as **Up**.

Example:

```
RP/0/RP0/CPU0:ios(config)#show ipv6 interface mgmtEth 0/RP0/CPU0/1 brief
Fri Oct 20 05:26:52.612 UTC
MgmtEth0/RP0/CPU0/1    [Up/Up]
    fe80::3afd:f8ff:fe66:872
    2001::1
```

Step 3 Run the **ipv6 access-list** command to configure an IPv6 ACL.

Example:

```
/* Configure an IPv6 ingress ACL */
RP/0/RP0/CPU0:ios(config)#ipv6 access-list V6-INGRESS-ACL
RP/0/RP0/CPU0:ios(config-ipv6-acl)#10 permit ipv6 any any
RP/0/RP0/CPU0:ios(config-ipv6-acl)#20 deny udp any any
RP/0/RP0/CPU0:ios(config-ipv6-acl)#commit
Fri Oct 20 05:28:46.664 UTC


/* Configure an IPv6 egress ACL */
Router(config)# ipv6 access-list V6-EGRESS-ACL
Router(config-ipv6-acl)# 10 permit ipv6 any any
Router(config-ipv6-acl)# 20 deny udp any any
Router(config-ipv6-acl)# commit
Thu Jul 11 09:50:40.566 UTC
```

Step 4 Run the **show access-lists ipv6** command to verify the ACL creation.

The entries highlighted in bold show the successful creation of ingress ACL and egresss ACL.

Example:

```
/* Verify the ingress ACL creation */
RP/0/RP0/CPU0:ios(config)# show access-lists ipv6
Fri Oct 20 05:29:01.125 UTC

ipv6 access-list V6-INGRESS-ACL
 10 permit ipv6 any any
 20 deny udp any any


/* Verify the egress ACL creation */
RP/0/RP0/CPU0:ios(config)# show access-lists ipv6
Fri Oct 20 05:29:01.125 UTC

ipv6 access-list V6-EGRESS-ACL
 10 permit ipv6 any any
 20 deny udp any any
```

Step 5 Run the **ipv6 access-group** command to apply the ACL to the management Ethernet interface.

Example:

```
/* Apply the ingress ACL to the mgmtEth interface */
RP/0/RP0/CPU0:ios(config)#interface mgmtEth 0/RP0/CPU0/1
RP/0/RP0/CPU0:ios(config-if)#ipv6 access-group V6-INGRESS-ACL ingress
RP/0/RP0/CPU0:ios(config-if)#commit
Fri Oct 20 05:37:32.738 UTC
RP/0/RP0/CPU0:ios(config-if)#exit


/* Apply the egress ACL to the mgmtEth interface */
Router(config)# interface mgmtEth 0/RP0/CPU0/1
Router(config-if)# ipv6 access-group V6-EGRESS-ACL egress
Router(config-if)# commit
Thu Jul 11 09:52:57.751 UTC
Router(config-if)# exit
```

Step 6 Run the **show ipv6 interface** command to verify whether the ACL has been successfully applied to the management Ethernet interface.

The entry highlighted in bold shows the ACL has been successfully applied to the management Ethernet interface.

Example:

```
/* Verify if the ingress ACL has been successfully applied to the mgmtEth interface */
RP/0/RP0/CPU0:ios#show ipv6 interface mgmtEth 0/RP0/CPU0/1
Fri Oct 20 05:38:00.753 UTC
MgmtEth0/RP0/CPU0/1 is Up, ipv6 protocol is Up, Vrfid is default (0x60000000)
  IPv6 is enabled, link-local address is fe80::3afd:f8ff:fe66:872
  Global unicast address(es):
    2001::1, subnet is 2001::/64
  Joined group address(es): ff02::1:ff00:1 ff02::1:ff66:872 ff02::2
      ff02::1
  MTU is 1514 (1500 is available to IPv6)
  ICMP redirects are disabled
  ICMP unreachables are enabled
  ND DAD is enabled, number of DAD attempts 1
  ND reachable time is 0 milliseconds
  ND cache entry limit is 1000000000
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 160 to 240 seconds
```

```
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses.
  Outgoing access list is not set
  Inbound  common access list is not set, access list is V6-INGRESS-ACL
  Table Id is 0xe0800000
  Complete protocol adjacency: 0
  Complete glean adjacency: 0
  Incomplete protocol adjacency: 0
  Incomplete glean adjacency: 0
  Dropped protocol request: 0
  Dropped glean request: 0
  RA DNS Server Address Count: 0
  RA DNS Search list Count: 0
/* Verify if the egress ACL has been successfully applied to the mgmtEth interface */

RP/0/RP0/CPU0:ios#show ipv6 interface mgmtEth 0/RP0/CPU0/1
Fri Oct 20 05:38:00.753 UTC
MgmtEth0/RP0/CPU0/1 is Up, ipv6 protocol is Up, Vrfid is default (0x60000000)
  IPv6 is enabled, link-local address is fe80::3afd:f8ff:fe66:872
  Global unicast address(es):
    2001::1, subnet is 2001::/64
  Joined group address(es): ff02::1:ff00:1 ff02::1:ff66:872 ff02::2
      ff02::1
  MTU is 1514 (1500 is available to IPv6)
  ICMP redirects are disabled
  ICMP unreachables are enabled
  ND DAD is enabled, number of DAD attempts 1
  ND reachable time is 0 milliseconds
  ND cache entry limit is 1000000000
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 160 to 240 seconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses.
  Outgoing access list is V6-EGRESS-ACL
  Inbound  common access list is not set, access list is not set
  Table Id is 0xe0800000
  Complete protocol adjacency: 0
  Complete glean adjacency: 0
  Incomplete protocol adjacency: 0
  Incomplete glean adjacency: 0
  Dropped protocol request: 0
  Dropped glean request: 0
  RA DNS Server Address Count: 0
  RA DNS Search list Count: 0
```

You have successfully configured an IPv6 standard ACL on the management Ethernet interface.

Configure an Extended Access Control List

To configure an extended ACL, you must create an ACL and specify the condition to allow or deny the network traffic.

Before you begin

Review the "Guidelines" and "Restrictions" sections of Access Control List, on page 1.

Step 1 Run the **ipv4 access-list** command to configure the ACL.

Example:

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#ipv4 access-list acl_1
```

Step 2 Run the **permit** and **deny** commands to specify the condition to allow or deny the network traffic

Example:

```
RP/0/RP0/CPU0:ios(config-ipv4-acl)#10 permit 172.16.0.0 0.0.255.255
RP/0/RP0/CPU0:ios(config-ipv4-acl)#20 deny 192.168.34.0 0.0.0.255
RP/0/RP0/CPU0:ios(config-ipv4-acl)#commit
```

Step 3 Run the **show access-lists** command to verify the ACL creation.

Example:

```
RP/0/RP0/CPU0:ios#show access-lists ipv4 acl_1
Fri Oct 20 06:22:17.223 UTC
ipv4 access-list acl_1
 10 permit ipv4 172.16.0.0 0.0.255.255 any
 20 deny ipv4 192.168.34.0 0.0.0.255 any
```

You have successfully configured an extended ACL on the management Ethernet interface.

Modify an Access Control List

Before you begin

Review the "Guidelines" and "Restrictions" sections of Access Control List, on page 1.

Step 1 Run the **ipv4 access-list** command to configure the ACL.

Example:

```
RP/0/RP0/CPU0:ios#configure
RP/0/RP0/CPU0:ios(config)#ipv4 access-list acl_1
```

Step 2 Run the **permit** command to add entries to the ACL.

Example:

```
RP/0/RP0/CPU0:ios(config-ipv4-acl)#10 permit ip host 10.3.3.3 host 172.16.5.34
RP/0/RP0/CPU0:ios(config-ipv4-acl)#20 permit icmp any any
RP/0/RP0/CPU0:ios(config-ipv4-acl)#30 permit tcp any host 10.3.3.3
RP/0/RP0/CPU0:ios(config-ipv4-acl)#end
```

Step 3 Run the **show access-lists** command to verify the ACL creation.

Example:

```
RP/0/RP0/CPU0:ios#show access-lists ipv4 acl_1
ipv4 access-list acl_1
10 permit ip host 10.3.3.3 host 172.16.5.34
20 permit icmp any any
30 permit tcp any host 10.3.3.3
```

Step 4 Run the **permit** command to modify the ACL.

Example:

```
*/Add new entries, one with a sequence number "15" and another without a sequence number to the ACL.
 Delete an entry with the sequence number "30":*/
RP/0/RP0/CPU0:ios(config)#ipv4 access-list acl_1
RP/0/RP0/CPU0:ios(config-ipv4-acl)# 15 permit 10.5.5.5 0.0.0.255
RP/0/RP0/CPU0:ios(config-ipv4-acl)# no 30
RP/0/RP0/CPU0:ios(config-ipv4-acl)# permit 10.4.4.4 0.0.0.255
RP/0/RP0/CPU0:ios(config-ipv4-acl)# commit
```

When an entry is added without a sequence number, it is automatically given a sequence number that puts it at the end of the access list. Because the default increment is 10, the entry will have a sequence number 10 higher than the last entry in the existing access list.

Step 5 Run the **show access-lists** command to verify the ACL creation.

Example:

```
RP/0/RP0/CPU0:ios#show access-lists ipv4 acl_1
ipv4 access-list acl_1
 10 permit ipv4 host 10.3.3.3 host 172.16.5.34

15 permit 10.5.5.5 0.0.0.255---*/newly added ACL (with the sequence number)*/
20 permit icmp any any
30 permit ipv4 10.4.4.0 0.0.0.255 any ---*/newly added ACL (without the sequence number)*/

*/The entry with the sequence number 30, that is, "30 permit tcp any host 10.3.3.3" is deleted from
 the ACL*/
```

You have successfully modified the ACL in operation.