Configure Access Control Lists

This procedure describes the access control lists (ACL) and the procedures to configure ACLs.

Table 1: Feature History

Feature Name	Release Information	Feature Description
ACL on Management Port	Cisco IOS XR Release 6.5.31	ACL allows you to control the packets that move through the network. This control allows you to limit the network traffic and restrict the access of users and devices to the network. NCS 4000 supports the following ACL: • ACL1—Ingress ACL on the out-of-band (OOB) management port

Table 2: Feature History

Feature Name	Release Information	Feature Description
ACL on Data Port	Cisco IOS XR Release 6.5.32	ACL allows you to control the packets that move through the network. This control allows you to limit the network traffic and restrict the access of users and devices to the network. ACL is supported on the data port.

Understanding ACL

ACLs perform packet filtering to control the packets that move through the network. These controls allow to limit the network traffic and restrict the access of users and devices to the network. ACLs have many uses, and therefore many commands accept a reference to an access list in their command syntax. An ACL consists of one or more access control entries (ACE) that collectively define the network traffic profile.

Purpose of ACLs

ACLs allow you to perform the following:

- 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.
- Control vty access.

How an ACL Works

An ACL is a sequential list consisting of permit and deny statements that apply to IP addresses and upper-layer IP protocols. The ACL has a name by which it is referenced. Many software commands accept an ACL as part of their syntax.

An ACL can be configured and named; however, it does not take effect until the ACL is referenced by a command that accepts an ACL. Multiple commands can reference the same ACL. An ACL can control traffic arriving at the router or leaving the router, but not traffic originating at the router.

Source address and destination address are two of the most typical fields in an IP packet on which to base an ACL. Specify source addresses to control packets from certain networking devices or hosts. Specify destination addresses to control packets that are sent to certain networking devices or hosts.

ACLs filter based on standard and extended ACLs to support the filtering of SSH, TACACs, DNS, NTP, ICMP, SNMP, and SYSLOG.

Support of ACLs

NCS 4000 supports the following ACL in R6.5.31:

- ACL1—Ingress IPv4 and IPv6 ACL on the out-of-band (OOB) management port.

NCS 4000 supports the following ACL in R6.5.32:

- Ingress IPv4 ACL on the data port.

Limitations of ACL on Management Port

The following limitations apply to ACL on the management port.

- Only IPv4 and IPv6 with ACL on the management port is supported.
- Ingress IPv4 and IPv6 with ACL on the management port is supported.
- Egress IPv4 and IPv6 with ACL on the management port is not supported.

Configure ACL on Management Port

This procedure describes how to configure the ACL on the IPv4 or IPv6 management port.

Procedure

Step 1 **configure**

Step 2 **interface** *interface-type Rack/Slot/Instance/Port*

Example:

```
RP/0/RP0:hostname(config)#
interface MgmtEth0/RP0/EMS/0
```

Enters interface configuration mode.

Step 3 **ipv4 | ipv6 access-group** *access-list-name* **ingress**

Example:

```
RP/0/RP0:hostname(config)#
ipv4 address 209.165.201.1 255.255.255.0
 ipv6 address 2001:db8::1/64
 ipv4 access-group EMS ingress
 ipv6 access-group EMS ingress
!
ipv4 access-list EMS
 10 permit udp any any
!
ipv6 access-list EMS
 10 permit udp any any
!
```

Configures ACL.

Step 4 **commit**

Verify ACL on Management Port

To verify the ACL configuration on the IPv4 or IPv6 management port, use the **show access-lists ipv4** or **show access-lists ipv6** commands.

Note Interface level filter for ACL statistics shows the entire line card statistics instead of specific interface statistics.

```
RP/0/RP0:hostname#show access-lists ipv4
ipv4 access-list CRAFT
10 deny icmp any any
ipv4 access-list EMS
10 deny icmp any any (200 matches)
```

Limitations of ACL on Data Port

The following limitations apply to ACL on the data port.

- Only IPv4 Ingress ACL is supported. IPv4 Egress, IPv6 Ingress, and IPv6 Egress are not supported.
- ACL permit statistics does not increment for the packets that are permitted and getting punted to CPU.
- QoS Ingress policy statistics does not work if ACL is applied on the same interface.
- ACL logging option is not supported.
- ACL fragments option and the ACL on fragmented packets are not supported.
- ACL filtering on BFD, BLB, and BoB packets are not supported.
- ACL statistics are reset to zero upon first read after RP switchover.

The following table describes the support matrix of ACL functional areas and fields.

Table 3: ACL Support Matrix

Area	Protocol or Feature	Direction	Details	Supported
General	IPv4 ACL	ingress	Only ingress IPv4 ACL is supported. No IPv6 support.	Y
Interface Type	IPv4 ACL	ingress	• Layer3 physical interfaces (main or bundle) • Layer3 subinterfaces (main or bundle)	Y

Area	Protocol or Feature	Direction	Details	Supported
Match Fields for IPv4 ACLs	IPv4 ACL			
	Src & Dst IP			Y
	L4 protocol			Y
	IP Prec			Y
	IP DSCP			Y
	L4 src & dst port – exact match			Y
	L4 src & dst port – range			Y
	Match on ICMP			Y
Actions	permit			Y
	deny			Y
Stats (Hit Count)	Both permit & deny			Y

Scale Information for ACL on Data Port

The following table describes the scale information for IPv4 ACL feature in ingress direction.

Table 4: Scale Information for ACL on Data Port

Parameter	Scale Details
Maximum unique ACLs per NPU	31
Maximum ACEs per NPU	300
Maximum permit or deny statistics per NPU	300

Configure ACL on IPv4 Data Port

This procedure describes how to configure the ACL on the IPv4 data port.

Procedure

Step 1 **configure**

Step 2 **interface** *interface-type Rack/Slot/Instance/Port*

Example:

```
RP/0/RP0:hostname(config)#
interface FortyGigE0/3/0/7
```

Enters interface configuration mode.

Step 3 **ipv4 address** *ipv4-address subnet-mask*

Example:

```
RP/0/RP0:hostname(config)#ipv4 address 100.1.6.2 255.255.255.252
```

Configures the IPv4 address and subnet mask.

Step 4 **ipv4 access-group** *access-list-name* **ingress**

Example:

```
RP/0/RP0:hostname(config)#ipv4 access-group test_scale_udp_generic ingress
```

Configures ACL.

Step 5 **commit**

Verify ACL on Data Port

To verify the ACL configuration on the data port, use the **show access-lists** command.

Note Interface level filter for ACL statistics shows the entire line card statistics instead of specific interface statistics.

```
RP/0/RP0:hostname#show access-lists test_ro_traffic_generic
Mon Jun 28 15:32:39.456 IST
ipv4 access-list test_RO_Traffic_Generic
10 permit tcp 100.1.0.0 0.0.255.255 eq bgp 100.1.0.0 0.0.255.255
20 permit tcp 100.1.0.0 0.0.255.255 100.1.0.0 0.0.255.255 eq bgp
30 permit udp 100.1.0.0 0.0.255.255 100.1.0.0 0.0.255.255 eq 6784
40 permit udp 100.1.0.0 0.0.255.255 eq ldp 100.1.0.0 0.0.255.255
50 permit udp 100.1.0.0 0.0.255.255 100.1.0.0 0.0.255.255 eq ldp
60 permit tcp 100.1.0.0 0.0.255.255 eq ldp 100.1.0.0 0.0.255.255
70 permit tcp 100.1.0.0 0.0.255.255 100.1.0.0 0.0.255.255 eq ldp
80 permit icmp 100.1.0.0 0.0.255.255 100.1.0.0 0.0.255.255
87 deny udp host 12.12.12.1 32.32.32.240 0.0.0.15 eq snmp
```

```
RP/0/RP0:hostname#show access-lists test_ro_traffic_generic hardware ingress location 0/lc0
Mon Jun 28 15:29:29.340 IST
ipv4 access-list test_scale_udp_generic
10 permit tcp 100.1.0.0 0.0.255.255 eq bgp 100.1.0.0 0.0.255.255
20 permit tcp 100.1.0.0 0.0.255.255 100.1.0.0 0.0.255.255 eq bgp
30 permit udp 100.1.0.0 0.0.255.255 100.1.0.0 0.0.255.255 eq 6784 (174370 matches)
40 permit udp 100.1.0.0 0.0.255.255 eq ldp 100.1.0.0 0.0.255.255
50 permit udp 100.1.0.0 0.0.255.255 100.1.0.0 0.0.255.255 eq ldp
60 permit tcp 100.1.0.0 0.0.255.255 eq ldp 100.1.0.0 0.0.255.255
70 permit tcp 100.1.0.0 0.0.255.255 100.1.0.0 0.0.255.255 eq ldp
80 permit icmp 100.1.0.0 0.0.255.255 100.1.0.0 0.0.255.255
87 deny udp host 12.12.12.1 32.32.32.240 0.0.0.15 eq snmp
```