Configuring IP ACLs

This chapter contains the following sections:

Information About ACLs

An access control list (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, the device tests the packet against the conditions of all rules. The rule determines whether the packet is to be permitted or denied. If there is no match to any of the specified rules, then the device denies the packet. The device continues processing packets that are permitted and drops packets that are denied.

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

ACL Types and Applications

An ACL is considered a port ACL when you apply it to one of the following:

- Ethernet interface
- vEthernet interface

When a port ACL is applied to a trunk port, the ACL filters traffic on all VLANs on that trunk port. Both IPv4 and IPv6 ACLs are supported.

Active Ports and Services on Nexus 1000V VSM

The following table lists the active ports and services on Nexus 1000V VSM:

Port Number	Protocol	Remark
22	SSH / SCP /SFTP (TCP)	
23	TELNET (TCP)	
123	NTP (UDP)	Used by NTP Sever
161	SNMP (UDP)	Used by SNMP Server

Order of ACL Application

When the device processes a packet, it determines the forwarding path of the packet. The device applies the ACLs in the following order:

1. Ingress port ACL
2. Egress port ACL

Rules

Rules are what you create, modify, and remove when you configure how an access control list (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 all VEMs.

You can create rules in ACLs 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 to match the rule.

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 IP or MAC ACLs. For information about specifying the source and destination, see the applicable permit and deny commands in the *Cisco Nexus 1000V Command reference* .

Protocols

ACLs allow you to identify traffic by protocol. You can specify some protocols by name. For example, in an IP ACL, you can specify ICMP by name.

In IP 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.

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.

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 1000V Command Reference* .

Implicit Rules

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. Implicit rules ensure that unmatched traffic is denied, regardless of the protocol specified in the Layer 2 header of the traffic.

All IPv4 ACLs include the following implicit rule that denies unmatched IP traffic:

```
deny ip any any
```

All IPv6 ACLs include the following implicit rule:

```
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 device permits neighbor discovery advertisement and solicitation messages. The fifth rule ensures that the device 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 rules.

All MAC ACLs include the following implicit rule:

```
deny any any
```

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:

- IP 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

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

See the *Cisco Nexus 1000V Command Reference* guide for information about filtering options available when using the applicable permit and deny commands.

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 by 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, you can 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.

Statistics

The device can maintain global statistics for each rule that you configure. 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.

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.

ACL Logging

You can use ACL logging to monitor flows that affect specific ACLs. The ACLs can be configured with the optional log keyword in each of the access control entries (ACEs). When you configure an option, statistics for each flow that match the ACL permit or deny conditions that you enter are logged in the software.

This example shows how to apply the log option to any IPv4 ACL:

```
switch(config)# ip access-list [name]
switch(config-acl)# permit tcp any 156.10.3.44/24 log
```

This example shows how to apply the log option to any IPv6 ACL:

```
switch(config)# ip access-list [name]
switch(config-acl)# permit tcp any 2001:0db8:85a3::/48 log
```

You can enable logging per rule(s) within the ACL. An implicit deny rule is the default action for ACLs. To log any packets that match the implicit deny rule, you must create an explicit deny rule and add the **log** keyword.

Note

- ACL logging is applicable only to IP ACLs that are configured with the **ip access-list** or **ipv6 access-list** commands. MAC ACL logging is not supported. Other traffic, such as the Virtual Supervisor Module (VSM) management interface or the selectors (aaa authen match, qos match, and so on), are not logged.
- ACL logging does not use the VSM management IP address. When in Layer 3 mode, ACL logging uses the Layer 3 vmk IP address. When in Layer 2 mode, ACL logging uses the vmk0 IP address.

Statistics and logging are provided for each flow. A flow is defined by the following IP flows:

- VSM ID
- Virtual Ethernet Module (VEM) ID
- Source interface
- Protocol
- Source IP address
- Source port
- Destination IP address

- Destination port

Scalability is provided through the following functionality:

- Each Cisco Nexus 1000V switch can support up to 256 VEMs.
- Each VEM can support up to 5000 permits and 5000 denies flows. The maximum number of permit/deny flows is a configurable option.
- The flow reporting interval can be set from 5 up to 86,400 seconds (1 day).
- The configuration flow syslog level can be from 0 to 7.
- Up to three syslog servers are supported.

ACL Flows

An ACL flow as it pertains to ACL logging has the following characteristics:

- It represents a stream of IPv4/IPv6 packets with the same packet headers (SrcIP, DstIP, Protocol, SrcPort, DstPort) for which an identical ACL action is enforced. Each flow entry tracks the count of packets that match the flow.
- It is created only if logging is enabled on the corresponding ingress/egress ACL policy. Ingress and egress flows are tracked separately.
- Each VEM tracks a maximum of 10,000 ACL flows; a flow space is shared between permit/deny flows, and each has a configurable maximum of 5000.
- Each flow entry contains the following:
  - Packet tuple
  - ACL action
  - Direction
  - Packet count
- The ACL flow life cycle is as follows:
  - A flow is created when the first packet of a unidirectional stream matches a Layer 3 ACL policy. A new flow notification is sent to the syslog server.
  - For all subsequent packets with a tuple that matches the flow tuple, the per flow packet counter is incremented.
  - Each flow is tracked periodically based on the configured reporting interval. Within each periodic report, all the active flows and the corresponding packet count seen since the last periodic report are reported to the syslog server
  - If no packets match a flow for one full periodic interval, the flow entry is purged. This process is the only flow-aging scheme.
  - A flow is not stateful. There is no connection tracking for TCP flows.
- The flow reporting process occurs in the following manner:

- For each flow created, a new flow notification message is sent to the syslog server.
- A periodic report for each active flow comes next. A flow is active if packets that match the flow are seen since the last periodic report.
- The flow information is exported to the syslog server and contains the following: packet tuple, ACL action, direction, VEM-ID, VSM-ID, packet count.
- The periodic time can be as low as 5 seconds with the default setting of 5 minutes. A new user space ACL-logging thread handles the periodic poll and report functionality.
- Syslog messages that identify the flow space usage are sent at 75 percent, 90 percent, and 100 percent of the threshold maximum to the syslog server once during each interval.

Syslog Messages

Syslog message characteristics are as follows:

- Syslog messages that contain flow information are exported from each Virtual Ethernet Module (VEM).
- The syslog client functionality is RFC-5424 compliant and communicates to servers over a UDP port (514).
- Any host that contains a VEM must be configured with a vmknic interface that can reach the remote syslog server.
- On an ESXi-5.0 host, syslog messages are blocked by a firewall. The Cisco Nexus 1000V has installation scripts that open the firewall for port 514.

Prerequisites for IP ACLs

- 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 for IP ACLs

ACLs are not supported in port channels.

Default Settings for IP ACLs

Parameters	Default
IP ACLs	No IP ACLs exist by default.
ACL rules	Implicit rules apply to all ACLs.

Configuring IP ACLs

Creating an IP ACL

You can create an IPv4 or IPv6 ACL on the device and add rules to it.

Before you begin

Log in to the CLI in EXEC mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **{ip | ipv6} access-list** *name*	Creates the named IP ACL (up to 64 characters) and enters IP ACL configuration mode.
Step 3	switch(config-acl)# [*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 from 1 to 4294967295. The **permit** and **deny** keywords support many ways of identifying traffic. For more information, see the *Cisco Nexus 1000V Command Reference*.
Step 4	(Optional) switch(config-acl)# **statistics per-entry**	Specifies that the device maintains global statistics for packets that match the rules in the ACL.
Step 5	(Optional) switch(config-acl)# **show** {**ip**|**ipv6**} **access-lists** *name*	Displays the IP ACL configuration.
Step 6	(Optional) switch(config-acl)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

This example shows how to create an IPv4 ACL:

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ip access-list acl-01
switch(config-acl)# permit ip 192.168.2.0/24 any
switch(config-acl)# statistics per-entry
switch(config-acl)# show ip access-lists acl-01
IPV4 ACL acl-01
        statistics per-entry
        10 permit ip 192.168.2.0/24 any
switch(config-acl)# copy running-config startup-config
```

This example shows how to create an IPv6 ACL:

```
switch# configure terminal
switch(config)# ipv6 access-list acl-01-ipv6
switch(config-ipv6-acl)# permit tcp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
```

Changing an IP ACL

You can add and remove rules in an existing IP ACL. You cannot change existing rules. Instead, to change a rule, you can remove it and create it again 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.

Before you begin

Log in to the CLI in EXEC mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# {**ip**|**ipv6**} **access-list** *name*	Places you in IP ACL configuration mode for the specified ACL.
Step 3	(Optional) switch(config-acl)# [*sequence-number*] {**permit** | **deny**} *protocol source destination*	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 from 1 to 4294967295. The **permit** and **deny** keywords support many ways of identifying traffic. For more information, see the *Cisco Nexus 1000V Command Reference*.
Step 4	(Optional) switch(config-acl)# **no** {*sequence-number* | {**permit** | **deny**} *protocol source destination}*	Removes the rule that you specified from the IP ACL. The **permit** and **deny** keywords support many ways of identifying traffic. For more information, see the *Cisco Nexus 1000V Command Reference*.
Step 5	(Optional) switch(config-acl)# [**no**] **statistics per-entry**	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	(Optional) switch(config-acl)# **show ip access-lists** *name*	Displays the IP ACL configuration.

	Command or Action	Purpose
Step 7	(Optional) switch(config-acl)# **copy running-config startup-config**	Copies the running configuration to the startup configuration
Step 8	(Optional) switch(config-acl)# **exit**	Exit the ACL configuration mode for the new rules to take effect. **Note** If you are not executing this step, then wait for 5 seconds for the new rules to take effect.

Example

This example shows how to change an IP ACL:

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ip access-list acl-01
switch(config-acl)# permit ip 192.168.2.0/24 any
switch(config-acl)# statistics per-entry
switch(config-acl)# show ip access-lists acl-01
IPV4 ACL acl-01
        statistics per-entry
        10 permit ip 192.168.2.0/24 any
switch(config-acl)# ip access-list acl-01
switch(config-acl)# no 10
switch(config-acl)# no statistics per-entry
switch(config-acl)# show ip access-lists acl-01

IPV4 ACL acl-01
switch(config-acl)# copy running-config startup-config
```

Removing an IP ACL

Before you remove an IP ACL from the switch, ensure that you know whether the ACL is applied to an interface. The switch 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 switch considers the removed ACL to be empty, that is, empty ACL with implicit rule of deny IP any .Use the **show ip access-lists** command with the summary keyword to find the interfaces that an IP ACL is configured on.

Before you begin

- Log in to the CLI in EXEC mode
- Know whether the ACL is applied to an interface.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.

	Command or Action	Purpose
Step 2	switch(config)# **no** {**ip**|**ipv6**} **access-list** *name*	Removes the IP ACL that you specified by name from the running configuration.
Step 3	(Optional) switch(config)# **show** {**ip**|**ipv6**} **access-list** *name* **summary**	Displays the IP ACL configuration. If the ACL remains applied to an interface, the command lists the interfaces.
Step 4	switch(config)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

This example shows how to remove an IP ACL:

```
switch# configure terminal
switch(config)# no ip access-list acl-01
switch(config)# show ip access-lists acl-01 summary
switch(config)# 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

Log in to the CLI in EXEC mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **resequence ip 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 from 1 to 4294967295.
Step 3	switch(config)# **show ip access-lists** *name*	Displays the IP ACL configuration.
Step 4	(Optional) switch(config)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

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

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# show ip access-lists acl-01
IPV4 ACL acl-01
        statistics per-entry
        10 permit ip 192.168.2.0/24 any
        20 permit ip 192.168.5.0/24 any
switch(config)# resequence ip access-list acl-01 100 10
switch(config)# show ip access-lists acl-01
IPV4 ACL acl-01
        statistics per-entry
        100 permit ip 192.168.2.0/24 any
        110 permit ip 192.168.5.0/24 any
switch(config)# copy running-config startup-config
```

Applying an IP ACL as a Port ACL

You can apply an IPv4 or IPv6 ACL to a physical Ethernet interface or a virtual Ethernet interface. ACLs applied to these interface types are considered port ACLs.

An IP ACL can also be applied on a port profile that is attached to a physical Ethernet interface or a virtual Ethernet interface.

Note ACLs cannot be applied on a port-channel interface. However, an ACL can be applied on a physical Ethernet interface that is not part of the port channel.

Before you begin

- Log in to the CLI in EXEC mode
- You can apply one port ACL to an interface.
- Check if the ACL that you want to apply exists and that it is configured to filter traffic in the manner that you need for this application.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface** {**vethernet** ¦ **ethernet**} *port*	Places you into interface configuration mode for the specified interface. **Note** Port ACLs are not supported on the port-channel interface and physical Ethernet interface that is a member of the port channel.

	Command or Action	Purpose
Step 3	switch(config-if)# {**ip port** | **ipv6 port**} {**access-group** | **traffic-filter**} *name* {**in** | **out**}	Adds the named IPv4 or IPv6 ACL to the port profile for either inbound or outbound traffic. You can apply only one IP port ACL to an interface.
Step 4	(Optional) switch(config-if)# **show running-config aclmgr**	Displays the ACL configuration.
Step 5	(Optional) switch(config-if)# **copy running-config startup-config**	Copies the running configuration to the startup configuration

Example

This example shows how to apply an IP ACL as a port ACL:

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# interface vethernet 1
switch(config-if)# ip port access-group acl-01 in
switch(config-if)# show running-config aclmgr
ip access-list acl-01
  statistics per-entry
  100 permit ip 192.168.2.0/24 any
  110 permit ip 192.168.5.0/24 any
interface Vethernet1
  ip port access-group acl-01 in
switch(config-if)# copy running-config startup-config
```

Adding an IP ACL to a Port Profile

You can add an IPv4 or IPv6 ACL to a port profile.

You must know the following information:

- If you want to create a new port profile, you must know the interface type (Ethernet or vEthernet) and the name you want to give the profile.
- The name of the IP access control list that you want to configure for this port profile.
- The direction of the packet flow for the access list.

Before you begin

- Log in to the CLI in EXEC mode.
- Create the IP ACL to add to this port profile and you know its name.
- If you are using an existing port profile, you have created it and you know its name.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **port-profile** [**type** {**ethernet** | **vethernet**}] *name*	Enters port profile configuration mode for the named port profile.
Step 3	switch(config-port-prof)# {**ip port** | **ipv6 port**} {**access-group** | **traffic-filter**} *name* { **in** | **out**}	Adds the named IPv4 or IPv6 ACL to the port profile for either inbound or outbound traffic.
Step 4	(Optional) switch(config-port-prof)# **show port-profile** [**brief** | **expand-interface** | **usage**] [**name** *profile-name*]	Displays the configuration for verification.
Step 5	(Optional) switch(config-port-prof)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

This example shows how to add an IP ACL to a port profile:

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# port-profile type vethernet vm_eth1
switch(config-port-prof)# ip port access-group acl-01 out
switch(config-port-prof)# show port-profile name vm_eth1
port-profile vm_eth1
 type: Vethernet
 description:
 status: enabled
 max-ports: 32
 min-ports: 1
 inherit:
 config attributes:
  ip port access-group acl-01 out
  no shutdown
 evaluated config attributes:
  ip port access-group acl-01 out
  no shutdown
 assigned interfaces:
 port-group: vm_eth1
 system vlans: none
 capability l3control: no
 capability iscsi-multipath: no
 capability vxlan: no
 capability l3-vn-service: no
 port-profile role: none
 port-binding: static

switch(config-port-prof)# copy running-config startup-config
```

Applying an IP ACL to the Management Interface

You can apply an IP ACL to the management interface, mgmt0.

Before you begin

Log in to the CLI in EXEC mode.

Be sure that the ACL that you want to apply exists and that it is configured to filter traffic in the manner that you need for this application.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface mgmt0**	Places you into interface configuration mode for the management interface.
Step 3	switch(config-if)# {**ip**|**ipv6**} **access-group | traffic-filter** *access-list* [**in** | **out**]	Applies a specified inbound or outbound IP ACL to the interface.
Step 4	(Optional) switch(config-if)# **show** {**ip**|**ipv6**} **access-group | traffic-filter** *access-list*	Displays the ACL configuration.
Step 5	switch(config-if)# {**ip**|**ipv6**} **access-list match-local-traffic**	The **match-local-traffic** option enables matching for locally-generated traffic. **Note** This global command has to be enabled for ACL rules to take effect when the ACL is applied in the egress direction on the mgmt 0 interface.
Step 6	(Optional) switch(config-if)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

This example shows how to apply an IP ACL to the management interface:

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ip access-list acl-01
switch(config-acl)# permit tcp any any
switch(config-acl)# show ip access-lists acl-01
IPV4 ACL acl-01
        10 permit tcp any any
switch(config-acl)# interface mgmt 0
switch(config-if)# ip access-group acl-01 out
switch(config-if)# show ip access-lists acl-01 summary
IPV4 ACL acl-01
        Total ACEs Configured:1
        Configured on interfaces:
                mgmt0 -  egress (Router ACL)
        Active on interfaces:
                mgmt0 -  egress (Router ACL)
switch(config-if)# ip access-list match-local-traffic
switch(config)# copy running-config startup-config
```

Configuring ACL Logging

ACL logging is enabled by default on all Virtual Ethernet Modules (VEMs). In addition, the following guidelines apply to ACL logging configuration:

- Any rule can be enabled for logging by adding the **log** keyword.
- Only packets that have a rule with the **log** keyword enabled are logged.

Disabling ACL Logging

You can disable ACL logging on a VEM by entering the following command:

Command	Purpose
[**no**] **logging ip access-list cache module** *vem*	Disables ACL logging on the specified VEM.

Configuring a Time Interval for Accumulating Packet Counters

You can configure the time interval for accumulating packet counters before they are reported to the syslog servers. You enter the time range in seconds from 5 to 86,400 seconds (1 day). The default is 300 seconds (5 minutes).

You can configure the amount of time to accumulate packet counters by entering one of the following commands:

Command	Purpose
logging ip access-list cache interval *secs*	Sets the time interval in seconds to accumulate packet counters before they are reported to the syslog servers, where *secs* is the number of seconds.
[**no**] **logging ip access-list cache interval** *secs*	Reverts the configuration to the default time interval configuration 300 seconds (5 minutes), where *secs* is the number of seconds.

These examples show the time interval syslog message format that is sent periodically when the time interval expires:

```
ACL-LOGGING-6-PERMIT-FLOW-INTERVAL <VSM-id> <VEM-id> <protocol> <source-interface>
 <source-ip/source-port)> <destination-ip/destination-port> Hit-count = <nnn>

ACL-LOGGING-6-DENY-FLOW-INTERVAL <VSM-id> <VEM-id> <protocol> <source-interface>
<source-ip/source-port)> <destination-ip/destination-port> Hit-count = <nnn>
```

Configuring Flows

You can configure the number of deny and permit flows per VEM. The range is from 0 to 5000 flows. The default is 3000. A syslog message is sent when the flow is near the maximum threshold. The first message is sent when the number of flows has reached 75 percent of the maximum threshold and the next message is sent when the number of flows has reached 90 percent of the maximum threshold. The last message is sent when the number of flows reaches the maximum threshold of 100 percent.

Configuring Permit Flows

You can configure permit flows by entering one of the following commands:

Command	Purpose
logging ip access-list cache max-permit-flows *num*	Sets the number of permit flows where *num* is the number of flows.
[**no**] **logging ip access-list cache max-permit-flows**	Reverts the configuration to the default permit flow value 3000.

These examples show permit flow syslog messages:

- New flow notification message:

```
-  Aug 28 04:17:19 fish-231-157.cisco.com 1 2011-08-28T11:14:23 - n1k-ecology -
ACLLOG-PERMIT-FLOW-CREATE VSM ID: 172.23.231.150, VEM ID:
86d04494-79e2-11df-a573-d0d0fd093c68, Source IP: 192.168.231.22, Destination IP:
192.168.231.21, Source Port: 42196, Destination Port: 8029, Source Interface: Veth2,
Protocol: "TCP"(6), Hit-count = 1
```

- Periodic flow reporting message:

```
-  Aug 28 04:17:20 sfish-231-157.cisco.com 1 2011-08-28T11:14:23 - n1k-acllog -
ACLLOG-PERMIT-FLOW-INTERVAL VSM ID: 172.23.231.150, VEM ID:
86d04494-79e2-11df-a573-d0d0fd093c68, Source IP: 192.168.231.22, Destination IP:
192.168.231.21, Source Port: 42196, Destination Port: 8029, Source Interface: Veth2,
Protocol: "TCP"(6), Hit-count = 1245
```

- Threshold crossing alarm messages:

```
-  Aug 28 04:17:22 sfish-231-157.cisco.com 1 2011-08-28T11:14:24 - n1k-acllog -
ACLLOG-MAX-PERMIT-FLOW-REACHED The number of ACL log permit-flows has reached 75 percent

limit (3969)
-  Aug 28 04:17:26 sfish-231-157.cisco.com 1 2011-08-28T11:14:26 - n1k-acllog -
ACLLOG-MAX-PERMIT-FLOW-REACHED The number of ACL log permit-flows has reached 90 percent

limit (4969)
-  Aug 28 04:17:27 sfish-231-157.cisco.com 1 2011-08-28T11:14:31 - n1k-acllog -
ACLLOG-MAX-PERMIT-FLOW-REACHED The number of ACL log permit-flows has reached 100 percent

limit (5000)
```

Configuring Deny Flows

You can configure deny flows by entering one of the following commands:

Command	Purpose
logging ip access-list cache max-deny-flows *num*	Sets the number of deny flows, where *num* is the number of flows.
[**no**] **logging ip access-list cache max-deny-flows**	Reverts the configuration back to the default deny flow value 3000.

These examples show deny flow syslog messages:

- New flow notification message

```
-  Aug 28 04:17:19 sfish-231-157.cisco.com 1 2011-08-28T11:14:23 - n1k-acllog -
ACLLOG-DENY-FLOW-CREATE VSM ID: 172.23.231.150, VEM ID:
86d04494-79e2-11df-a573-d0d0fd093c68, Source IP: 192.168.231.22, Destination IP:
192.168.231.100, Source Port: 48528, Destination Port: 8029, Source Interface: Veth2,
Protocol: "TCP"(6), Hit-count = 1
```

- Periodic flow reporting message

```
-  Aug 28 04:17:20 sfish-231-157.cisco.com 1 2011-08-28T11:14:23 - n1k-acllog -
ACLLOG-DENY-FLOW-INTERVAL VSM ID: 172.23.231.150, VEM ID:
86d04494-79e2-11df-a573-d0d0fd093c68, Source IP: 192.168.231.22, Destination IP:
192.168.231.100, Source Port: 47164, Destination Port: 8029, Source Interface: Veth2,
Protocol: "TCP"(6), Hit-count = 1245
```

- Threshold crossing alarm messages

```
-  Aug 28 04:17:27 sfish-231-157.cisco.com 1 2011-08-28T11:14:31 - n1k-acllog -
ACLLOG-MAX-DENY-FLOW-REACHED The number of ACL log deny-flows has reached 75 percent
limit
(4330)
-  Aug 28 04:18:27 sfish-231-157.cisco.com 1 2011-08-28T11:15:31 - n1k-acllog -
ACLLOG-MAX-DENY-FLOW-REACHED The number of ACL log deny-flows has reached 90 percent
limit
(4630)
-  Aug 28 04:20:17 sfish-231-157.cisco.com 1 2011-08-28T11:17:20 - n1k-acllog -
ACLLOG-MAX-PERMIT-FLOW-REACHED The number of ACL log permit-flows has reached 100 percent

limit (5000)
```

Syslog Server Severity Levels

You can configure severity levels of the ACL logging syslog messages for up to three remote syslog servers. The range is from 0 to 7. The default severity level is 6.

Severity Code	Severity Level	Description
0	Emergency	System is unusable
1	Alert	Action must be taken immediately
2	Critical	Critical conditions
3	Error	Error conditions
4	Warning	Warning conditions
5	Notice	Normal but significant condition
6	Informational	informational messages
7	Debug	Debug-level messages

Setting the Severity Level for a Syslog Message

You can set the severity level of a syslog message and the server to which you want the message to be sent by entering one of the following commands:

Command	Purpose
[**no**] **acllog match-log-level** *level*	Sets the severity level at which syslog messages are sent, where *level* is the severity code from 0 to 7. The no acllog match-log-level level command will revert the ACL log level back to the default severity level 6.
[**no**] **logging ip access-list cache max-deny-flows** *number*	Sets the maximum number of deny flows to *number* per module. The **no logging ip access-list cache max-deny-flows** *number* sets the maximum number of deny-flows to default value of 3000.
[**no**] **logging ip access-list cache max-permit-flows** *number*	Set the max-permit-flows to a specified number per module. The **no logging ip access-list cache max-permit-flows** *number* sets the maximum number of permit-flows to default value of 3000.
logging server { *A.B.C.D* | *x:x:x:x:x:x:x:x*}*-level*	Specifies the syslog server on which you want to set a severity level, where *A.B.C.D* is the syslog server IPv4 address and *x:x:x:x:x:x:x:x* is the syslog server IPv6 address. The severity levels are between 0 to 7.

Note For ACL logging to work, ACL Logging level should be equal or less than that of Syslog level.

Verifying the IP ACL Configuration

Use one of the following commands to verify the configuration:

Command	Purpose
show running-config aclmgr	Displays the ACL configuration, including the IP ACL configuration and interfaces that IP ACLs are applied to.
show {**ip**|**ipv6**} **access-lists** [*name*]	Displays all IP ACLs or a named IP ACL.
show {**ip**|**ipv6**} **access-lists** [*name*] su**mmary**	Displays a summary of all configured IP ACLs or a named IP ACL.
show running-config interface	Displays the configuration of an interface to which you have applied an ACL.
show logging ip access-list status	Displays the ACL logging configuration for a VSM.
vemcmd show acllog config	Displays the VEM ACL logging configuration.

Monitoring IP ACLs

Use one of the following commands for IP ACL monitoring:

Command	Purpose
show {**ip**|**ipv6**} **access-lists**	Displays the IPv4 or IPv6 ACL configuration. If the IP ACL includes the **statistics per-entry** command, the output includes the number of packets that have matched each rule.
clear {**ip**|**ipv6**} **access-list** [*name*] **counters**	Clears statistics for all IPv4 or IPv6 ACLs or for a specific IPv4 or IPv6 ACL.

Configuration Example for IP ACL

This example shows how to create an IPv4 ACL named acl-01 and apply it as a port ACL on physical ethernet interface which is not a member of port-channel and configuration verification with match counters:

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ip access-list acl-01
switch(config-acl)# permit ip 192.168.2.0/24 any
switch(config-acl)# permit ip 192.168.5.0/24 any
switch(config-acl)# permit 22 any 10.105.225.225/27
switch(config-acl)# permit ip any 10.105.225.225/27
switch(config-acl)# statistics per-entry
switch(config-acl)# interface ethernet 3/5
switch(config-if)# ip port access-group acl-01 in
switch(config-if)# show ip access-lists acl-01 summary
IPV4 ACL acl-01
        statistics per-entry
        Total ACEs Configured:4
        Configured on interfaces:
                Ethernet3/5 - ingress (Port ACL)
        Active on interfaces:
                Ethernet3/5 - ingress (Port ACL)
switch(config-if)# show ip access-lists acl-01
IPV4 ACL acl-01
        statistics per-entry
        100 permit ip 192.168.2.0/24 any [match=0]
        110 permit ip 192.168.5.0/24 any [match=0]
        120 permit 22 any 10.105.225.225/27 [match=0]
        130 permit ip any 10.105.225.225/27 [match=44]
switch(config-if)# clear ip access-list counters acl-01
switch(config-if)# show ip access-lists acl-01
IPV4 ACL acl-01
        statistics per-entry
        100 permit ip 192.168.2.0/24 any [match=0]
        110 permit ip 192.168.5.0/24 any [match=0]
        120 permit 22 any 10.105.225.225/27 [match=0]
        130 permit ip any 10.105.225.225/27 [match=0]
switch(config-if)#
```

This example shows how to enable access list matching for locally generated traffic:

```
switch# ip access-list match-local-traffic
```

This example shows how to verify VSM ACL logging configuration:

```
switch# show logging ip access-list status
Max deny flows = 3000
Max permit flows = 3000
Alert interval = 300
Match log level = 6
VSM IP = 192.168.1.1
Syslog IP = 10.1.1.1
Syslog IP = 0.0.0.0
Syslog IP = 0.0.0.0
ACL Logging enabled on module(s):
4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19
20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35
36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51
52 53 54 55 56 57 58 59 60 61 62 63 64 65 66
ACL Logging disabled on module(s):
3
```

This example shows how to verify VEM ACL logging configuration:

```
switch# vemcmd show acllog config
ACL-Log Config:
Status: enabled
Reporting Interval: 300
Max Permit Flows: 3000
Max Deny Flows: 3000
Syslog Facility : 4
Syslog Severity: 6
Syslog Srvr 1: 10.1.1.1
Syslog Srvr 2: 0.0.0.0
Syslog Srvr 3: 0.0.0.0
VSM: 192.168.1.1
```

Feature History for IP ACLs

This table only includes updates for those releases that have resulted in additions to the feature.

Feature History	Releases	Feature Information
IPv6 ACLs	5.2(1)SV3(1.1)	This feature was introduced.
IPv6 ACL Logging	5.2(1)SV3(1.1)	
IPv4 ACL Logging	4.2(1)SV1(5.1)	This feature was introduced.
IP ACLs for mgmt0 interface	4.2(1) SV1(4)	This feature was introduced.
IP ACLs	4.0(4)SV1(1)	This feature was introduced.