



Configuring IPv6 ACL

- [Finding Feature Information, page 1](#)
- [Information About Configuring IPv6 ACLs, page 1](#)
- [Configuring IPv6 ACLs, page 3](#)
- [Configuration Examples for IPv6 ACL, page 9](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Information About Configuring IPv6 ACLs

You can filter IP version 6 (IPv6) traffic by creating IPv6 access control lists (ACLs) and applying them to interfaces similarly to the way that you create and apply IP version 4 (IPv4) named ACLs. You can also create and apply input router ACLs to filter Layer 3 management traffic.



Note

To use IPv6, you must configure the dual IPv4 and IPv6 Switch Database Management (SDM) template on the switch. You select the template by entering the **sdm prefer {default | dual-ipv4-and-ipv6}** global configuration command.



Note

For complete syntax and usage information for the commands used in this chapter, see the command reference for this release or the Cisco IOS documentation referenced in the procedures.

Understanding IPv6 ACLs

A switch image supports two types of IPv6 ACLs:

- IPv6 router ACLs - Supported on outbound or inbound traffic on Layer 3 interfaces, which can be routed ports, switch virtual interfaces (SVIs), or Layer 3 EtherChannels. Applied to only IPv6 packets that are routed.
- IPv6 port ACLs - Supported on inbound traffic on Layer 2 interfaces only. Applied to all IPv6 packets entering the interface.



Note

If you configure unsupported IPv6 ACLs, an error message appears and the configuration does not take affect.

The switch does not support VLAN ACLs (VLAN maps) for IPv6 traffic.

You can apply both IPv4 and IPv6 ACLs to an interface.

As with IPv4 ACLs, IPv6 port ACLs take precedence over router ACLs:

- When an input router ACL and input port ACL exist in an SVI, packets received on ports to which a port ACL is applied are filtered by the port ACL. Routed IP packets received on other ports are filtered by the router ACL. Other packets are not filtered.
- When an output router ACL and input port ACL exist in an SVI, packets received on the ports to which a port ACL is applied are filtered by the port ACL. Outgoing routed IPv6 packets are filtered by the router ACL. Other packets are not filtered.



Note

If any port ACL (IPv4, IPv6, or MAC) is applied to an interface, that port ACL is used to filter packets, and any router ACLs attached to the SVI of the port VLAN are ignored.

Supported ACL Features

IPv6 ACLs on the switch have these characteristics:

- Fragmented frames (the fragments keyword as in IPv4) are supported.
- The same statistics supported in IPv4 are supported for IPv6 ACLs.
- If the switch runs out of TCAM space, packets associated with the ACL label are forwarded to the CPU, and the ACLs are applied in software.
- Routed or bridged packets with hop-by-hop options have IPv6 ACLs applied in software.
- Logging is supported for router ACLs, but not for port ACLs.
- The switch supports IPv6 address-matching for a full range of prefix lengths.

IPv6 ACL Limitations

With IPv4, you can configure standard and extended numbered IP ACLs, named IP ACLs, and MAC ACLs. IPv6 supports only named ACLs.

The switch supports most Cisco IOS-supported IPv6 ACLs with some exceptions:

- IPv6 source and destination addresses-ACL matching is supported only on prefixes from /0 to /64 and host addresses (/128) that are in the extended universal identifier (EUI)-64 format. The switch supports only these host addresses with no loss of information:
 - aggregatable global unicast addresses
 - link local addresses
- The switch does not support matching on these keywords: **flowlabel**, **routing header**, and **undetermined-transport**.
- The switch does not support reflexive ACLs (the **reflect** keyword).
- This release supports only port ACLs and router ACLs for IPv6; it does not support VLAN ACLs (VLAN maps).
- The switch does not apply MAC-based ACLs on IPv6 frames.
- You cannot apply IPv6 port ACLs to Layer 2 EtherChannels.
- The switch does not support output port ACLs.
- Output router ACLs and input port ACLs for IPv6 are supported only on . Switches support only control plane (incoming) IPv6 ACLs.
- When configuring an ACL, there is no restriction on keywords entered in the ACL, regardless of whether or not they are supported on the platform. When you apply the ACL to an interface that requires hardware forwarding (physical ports or SVIs), the switch checks to determine whether or not the ACL can be supported on the interface. If not, attaching the ACL is rejected.
- If an ACL is applied to an interface and you attempt to add an access control entry (ACE) with an unsupported keyword, the switch does not allow the ACE to be added to the ACL that is currently attached to the interface.

Configuring IPv6 ACLs

Before configuring IPv6 ACLs, you must select one of the dual IPv4 and IPv6 SDM templates.

To filter IPv6 traffic, you perform these steps:

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|--|---------|
| Step 1 | Create an IPv6 ACL, and enter IPv6 access list configuration mode. | |
| Step 2 | Configure the IPv6 ACL to block (deny) or pass (permit) traffic. | |

| | Command or Action | Purpose |
|--------|--|---------|
| Step 3 | Apply the IPv6 ACL to an interface. For router ACLs, you must also configure an IPv6 address on the Layer 3 interface to which the ACL is applied. | |

Default IPv6 ACL Configuration

There are no IPv6 ACLs configured or applied.

Interaction with Other Features and Switches

- If an IPv6 router ACL is configured to deny a packet, the packet is not routed. A copy of the packet is sent to the Internet Control Message Protocol (ICMP) queue to generate an ICMP unreachable message for the frame.
- If a bridged frame is to be dropped due to a port ACL, the frame is not bridged.
- You can create both IPv4 and IPv6 ACLs on a switch or switch stack, and you can apply both IPv4 and IPv6 ACLs to the same interface. Each ACL must have a unique name; an error message appears if you try to use a name that is already configured.

You use different commands to create IPv4 and IPv6 ACLs and to attach IPv4 or IPv6 ACLs to the same Layer 2 or Layer 3 interface. If you use the wrong command to attach an ACL (for example, an IPv4 command to attach an IPv6 ACL), you receive an error message.

- You cannot use MAC ACLs to filter IPv6 frames. MAC ACLs can only filter non-IP frames.
- If the hardware memory is full, for any additional configured ACLs, packets are dropped to the CPU, and the ACLs are applied in software. When the hardware is full a message is printed to the console indicating the ACL has been unloaded and the packets will be dropped on the interface.



Note Only packets of the same type as the ACL that could not be added (ipv4, ipv6, MAC) will be dropped on the interface.

Creating IPv6 ACL

Beginning in privileged EXEC mode, follow these steps to create an IPv6 ACL:

DETAILED STEPS

| | Command or Action | Purpose |
|--------|--|--|
| Step 1 | <p>configure terminal</p> <p>Example: SwitchControllerDevice# configure terminal</p> | Enters global configuration mode. |
| Step 2 | <p>ipv6access-list<i>access-list-name</i></p> <p>Example: ipv6 access-list access-list-name</p> | Define an IPv6 access list name, and enter IPv6 access-list configuration mode. |
| Step 3 | <p>{deny permit} protocol</p> <p>Example: {deny permit} protocol {source-ipv6-prefix/prefix-length any host source-ipv6-address} [operator [port-number]][destination-ipv6-prefix/prefix-length any host destination-ipv6-address] [operator [port-number]][dscp value] [fragments][log [log-input] [routing][sequence value] [time-range name]</p> | <p>Enter deny or permit to specify whether to deny or permit the packet if conditions are matched. These are the conditions:</p> <ul style="list-style-type: none"> • For protocol, enter the name or number of an Internet protocol: ahp, esp, icmp, ipv6, pcp, stcp, tcp, or udp, or an integer in the range 0 to 255 representing an IPv6 protocol number. • The source-ipv6-prefix/prefix-length or destination-ipv6-prefix/ prefix-length is the source or destination IPv6 network or class of networks for which to set deny or permit conditions, specified in hexadecimal and using 16-bit values between colons (see RFC 2373). • Enter any as an abbreviation for the IPv6 prefix ::/0. • For host source-ipv6-address or destination-ipv6-address, enter the source or destination IPv6 host address for which to set deny or permit conditions, specified in hexadecimal using 16-bit values between colons. • (Optional) For operator, specify an operand that compares the source or destination ports of the specified protocol. Operands are lt (less than), gt (greater than), eq (equal), neq (not equal), and range. <p>If the operator follows the source-ipv6-prefix/prefix-length argument, it must match the source port. If the operator follows the destination-ipv6- prefix/prefix-length argument, it must match the destination port.</p> <ul style="list-style-type: none"> • (Optional) The port-number is a decimal number from 0 to 65535 or the name of a TCP or UDP port. You can use TCP port names only when filtering TCP. You can use UDP port names only when filtering UDP. • (Optional) Enter dscp value to match a differentiated services code point value against the traffic class value in the Traffic Class field of each IPv6 packet header. The acceptable range is from 0 to 63. |

| | Command or Action | Purpose |
|---------------|--|--|
| | | <ul style="list-style-type: none"> • (Optional) Enter fragments to check noninitial fragments. This keyword is visible only if the protocol is ipv6. • (Optional) Enter log to cause an logging message to be sent to the console about the packet that matches the entry. Enter log-input to include the input interface in the log entry. Logging is supported only for router ACLs. • (Optional) Enter routing to specify that IPv6 packets be routed. • (Optional) Enter sequence value to specify the sequence number for the access list statement. The acceptable range is from 1 to 4294967295 • (Optional) Enter time-range name to specify the time range that applies to the deny or permit statement. |
| Step 4 | <p>{deny permit} tcp</p> <p>Example:</p> <pre>{deny permit} tcp {source-ipv6-prefix/prefix-length any hostsource-ipv6-address} [operator [port-number]]{destination-ipv6-prefix/prefix-length any hostdestination-ipv6-address} [operator [port-number]][ack] [dscp value][established] [fin] [log][log-input] [neq {port protocol}] [psh] [range{port protocol}] [rst][routing] [sequence value] [syn] [time-range name][urg]</pre> | <p>(Optional) Define a TCP access list and the access conditions. Enter tcp for Transmission Control Protocol. The parameters are the same as those described in Step 3, with these additional optional parameters:</p> <ul style="list-style-type: none"> • ack—Acknowledgment bit set. • established—An established connection. A match occurs if the TCP datagram has the ACK or RST bits set. • fin—Finished bit set; no more data from sender. • neq {port protocol}—Matches only packets that are not on a given port number. • psh—Push function bit set. • range {port protocol}—Matches only packets in the port number range. • rst—Reset bit set. • syn—Synchronize bit set. • urg—Urgent pointer bit set. |
| Step 5 | <p>{deny permit} udp</p> <p>Example:</p> <pre>{deny permit} udp {source-ipv6-prefix/prefix-length any hostsource-ipv6-address} [operator [port-number]]{destination-ipv6-prefix/prefix-length any hostdestination-ipv6-address} [operator [port-number]][dscp value] [log][log-input]</pre> | <p>(Optional) Define a UDP access list and the access conditions. Enter udp for the User Datagram Protocol. The UDP parameters are the same as those described for TCP, except that the operator [port]] port number or name must be a UDP port number or name, and the established parameter is not valid for UDP.</p> |

| | Command or Action | Purpose |
|---------------|---|---|
| | <code>[neg {port protocol}] [range {port protocol}] [routing] [sequence value] [time-range name]</code> | |
| Step 6 | <p>{deny permit} icmp</p> <p>Example:</p> <pre>{deny permit} icmp {source-ipv6-prefix/prefix-length any hostsource-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/prefix-length any hostdestination-ipv6-address} [operator [port-number]][icmp-type [icmp-code] icmp-message] [dscpvalue] [log] [log-input] [routing] [sequence value][time-range name]</pre> | <p>(Optional) Define an ICMP access list and the access conditions.</p> <p>Enter icmp for Internet Control Message Protocol. The ICMP parameters are the same as those described for most IP protocols in Step 3a, with the addition of the ICMP message type and code parameters. These optional keywords have these meanings:</p> <ul style="list-style-type: none"> • icmp-type—Enter to filter by ICMP message type, a number from 0 to 255. • icmp-code—Enter to filter ICMP packets that are filtered by the ICMP message code type, a number from 0 to 255. • icmp-message—Enter to filter ICMP packets by the ICMP message type name or the ICMP message type and code name. To see a list of ICMP message type names and code names, use the ? key or see command reference for this release. |
| Step 7 | <p>end</p> <p>Example:</p> <pre>SwitchControllerDevice(config)# end</pre> | Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode. |
| Step 8 | <p>show ipv6 access-list</p> <p>Example:</p> <pre>show ipv6 access-list</pre> | Verify the access list configuration. |
| Step 9 | <p>copy running-config startup-config</p> <p>Example:</p> <pre>copy running-config startup-config</pre> | (Optional) Save your entries in the configuration file. |

Applying an IPv6 ACL to an Interface

This section describes how to apply IPv6 ACLs to network interfaces. You can apply an ACL to outbound or inbound traffic on Layer 3 interfaces, or to inbound traffic on Layer 2 interfaces.

Beginning in privileged EXEC mode, follow these steps to control access to an interface:

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | configure terminal Example: SwitchControllerDevice# configure terminal | Enters global configuration mode. |
| Step 2 | interface interface_id Example: SwitchControllerDevice# interface interface-id | Identify a Layer 2 interface (for port ACLs) or Layer 3 interface (for router ACLs) on which to apply an access list, and enter interface configuration mode. |
| Step 3 | no switchport Example: SwitchControllerDevice# no switchport | If applying a router ACL, change the interface from Layer 2 mode (the default) to Layer 3 mode. |
| Step 4 | ipv6 address ipv6_address Example: SwitchControllerDevice# ipv6 address ipv6-address | Configure an IPv6 address on a Layer 3 interface (for router ACLs). This command is not required on Layer 2 interfaces or if the interface has already been configured with an explicit IPv6 address. |
| Step 5 | ipv6 traffic-filter access-list-name Example: SwitchControllerDevice# ipv6 traffic-filter access-list-name {in out} | Apply the access list to incoming or outgoing traffic on the interface. The out keyword is not supported for Layer 2 interfaces (port ACLs). |
| Step 6 | end Example: SwitchControllerDevice(config)# end | Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode. |
| Step 7 | show running-config | Verify the access list configuration. |
| Step 8 | copy running-config startup-config Example: copy running-config startup-config | (Optional) Saves your entries in the configuration file. |

Displaying IPv6 ACLs

You can display information about all configured access lists, all IPv6 access lists, or a specific access list by using one or more of the privileged EXEC commands.

DETAILED STEPS

| | Command or Action | Purpose |
|--------|--|--|
| Step 1 | show access-list Example: SwitchControllerDevice# show access-lists | Displays all access lists configured on the switchcontrollerdevice |
| Step 2 | show ipv6 access-list <i>acl_name</i> Example: SwitchControllerDevice# show ipv6 access-list [<i>access-list-name</i>] | Displays all configured IPv6 access list or the access list specified by name. |

Configuration Examples for IPv6 ACL

Example: Creating IPv6 ACL

This example configures the IPv6 access list named CISCO. The first deny entry in the list denies all packets that have a destination TCP port number greater than 5000. The second deny entry denies packets that have a source UDP port number less than 5000. The second deny also logs all matches to the console. The first permit entry in the list permits all ICMP packets. The second permit entry in the list permits all other traffic. The second permit entry is necessary because an implicit deny -all condition is at the end of each IPv6 access list.


Note

Logging is supported only on Layer 3 interfaces.

```
SwitchControllerDevice(config)# ipv6 access-list CISCO
SwitchControllerDevice(config-ipv6-acl)# deny tcp any any gt 5000
SwitchControllerDevice (config-ipv6-acl)# deny ::/0 lt 5000 ::/0 log
SwitchControllerDevice(config-ipv6-acl)# permit icmp any any
SwitchControllerDevice(config-ipv6-acl)# permit any any
```

Example: Applying IPv6 ACLs

This example shows how to apply the access list Cisco to outbound traffic on a Layer 3 interface.

```
SwitchControllerDevice(config)# interface TenGigabitEthernet 1/0/3
SwitchControllerDevice(config-if)# no switchport
SwitchControllerDevice(config-if)# ipv6 address 2001::/64 eui-64
SwitchControllerDevice(config-if)# ipv6 traffic-filter CISCO out
```

Example: Displaying IPv6 ACLs

This is an example of the output from the **show access-lists** privileged EXEC command. The output shows all access lists that are configured on the switch or switch stack.

```
SwitchControllerDevice #show access-lists
Extended IP access list hello
10 permit ip any any
IPv6 access list ipv6
permit ipv6 any any sequence 10
```

This is an example of the output from the **show ipv6 access-lists** privileged EXEC command. The output shows only IPv6 access lists configured on the switch or switch stack.

```
SwitchControllerDevice# show ipv6 access-list
IPv6 access list inbound
permit tcp any any eq bgp (8 matches) sequence 10
permit tcp any any eq telnet (15 matches) sequence 20
permit udp any any sequence 30

IPv6 access list outbound
deny udp any any sequence 10
deny tcp any any eq telnet sequence 20
```