IPv6 Services—Standard Access Control Lists

Access lists determine the type of traffic that is blocked or forwarded at device interfaces. Access control lists (ACLs) allow the filtering of inbound and outbound traffic at interfaces based on source and destination addresses.

This module provides information about standard IPv6 ACLs.

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.

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

Information About IPv6 Services--Standard Access Control Lists

Access Control Lists for IPv6 Traffic Filtering

The standard ACL functionality in IPv6 is similar to standard ACLs in IPv4. Access lists determine what traffic is blocked and what traffic is forwarded at device interfaces and allow filtering based on source and destination addresses, inbound and outbound to a specific interface. Each access list has an implicit deny

statement at the end. IPv6 ACLs are defined and their deny and permit conditions are set using the **ipv6 access-list**command with the **deny** and **permit** keywords in global configuration mode.

IPv6 extended ACLs augments standard IPv6 ACL functionality to support traffic filtering based on IPv6 option headers and optional, upper-layer protocol type information for finer granularity of control (functionality similar to extended ACLs in IPv4).

IPv6 Packet Inspection

The following header fields are used for IPv6 inspection: traffic class, flow label, payload length, next header, hop limit, and source or destination IP address. For further information on and descriptions of the IPv6 header fields, see RFC 2474.

Access Class Filtering in IPv6

Filtering incoming and outgoing connections to and from the device based on an IPv6 ACL is performed using the **ipv6 access-class** command in line configuration mode. The **ipv6 access-class** command is similar to the **access-class** command, except the IPv6 ACLs are defined by a name. If the IPv6 ACL is applied to inbound traffic, the source address in the ACL is matched against the incoming connection source address and the destination address in the ACL is matched against the local device address on the interface. If the IPv6 ACL is applied to outbound traffic, the source address in the ACL is matched against the local device address on the interface and the destination address in the ACL is matched against the outgoing connection source address. We recommend that identical restrictions are set on all the virtual terminal lines because a user can attempt to connect to any of them.

How to Configure IPv6 Services--Standard Access Control Lists

Configuring IPv6 Services—Standard Access Control Lists

IPv6 access control lists (ACLs) do not contain implicit permit rules.

The IPv6 neighbor discovery process uses the IPv6 network-layer service; therefore, you must configure IPv6 ACLs to allow IPv6 neighbor discovery packets to be sent and received on an interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 access-list** *access-list-name*
4. **permit** *source-ipv6-prefix*/*prefix-length* **host**
5. **deny** *protocol source-ipv6-prefix*/*prefix-length* **eq telnet any**
6. **exit**
7. **interface** *type number*
8. **ipv6 traffic-filter** *access-list-name* {**in** | **out**}
9. **end**
10. **show ipv6 access-list** [*access-list-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 access-list** *access-list-name* **Example:** `Device(config)# ipv6 access-list ipv6acl`	Defines an IPv6 ACL and enters IPv6 access list configuration mode. • IPv6 ACL names cannot contain a space or quotation mark or begin with a numeral.
Step 4	**permit** *source-ipv6-prefix*/*prefix-length* **host** **Example:** `Device(config-ipv6-acl)# permit 2001:DB8:1::1/32 any`	Specifies permit conditions for the IPv6 access list.
Step 5	**deny** *protocol source-ipv6-prefix*/*prefix-length* **eq telnet any** **Example:** `Device(config-ipv6-acl)# deny tcp 2001:DB8:0300:0201::/32 eq telnet any`	Specifies deny conditions for the IPv6 access list.

	Command or Action	Purpose
Step 6	**exit** **Example:** `Device(config-ipv6-acl)# exit`	Exits IPv6 access list configuration mode and enters global configuration mode.
Step 7	**interface** *type number* **Example:** `Device(config)# interface Gigabitethernet 1/0/2`	Configures an interface and enters interface configuration mode.
Step 8	**ipv6 traffic-filter** *access-list-name* {**in** | **out**} **Example:** `Device(config-if)# ipv6 traffic-filter ipv6acl out`	Applies the specified IPv6 access list to the interface configured in Step 7.
Step 9	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and enters privileged EXEC mode.
Step 10	**show ipv6 access-list** [*access-list-name*] **Example:** `Device# show ipv6 access-list`	Displays the contents of all current IPv6 access lists.

Example:

The following is sample output from the **show ipv6 access-list** command:

```
Device# show ipv6 access-list

IPv6 access list ipv6acl
    permit tcp any any eq bgp reflect tcptraffic (8 matches) sequence 10
    permit tcp any any eq telnet reflect tcptraffic (15 matches) sequence 20
    permit udp any any reflect udptraffic sequence 30

IPv6 access list tcptraffic (reflexive) (per-user)
    permit tcp host 2001:DB8:1::32 eq bgp host 2001:DB8:2::32 eq 11000 timeout 300 (time
left 243) sequence 1
    permit tcp host 2001:DB8:1::32 eq telnet host 2001:DB8:2::32 eq 11001 timeout 300 (time
 left 296) sequence 2

IPv6 access list outbound
    evaluate udptraffic
    evaluate tcptraffic
```

Configuration Examples for IPv6 Services--Standard Access Control Lists

Example: Configuring IPv6 Services—Standard Access Control Lists

```
Device# configure terminal
Device(config)# ipv6 access-list ipv6acl
Device(config-ipv6-acl)# permit 2001:DB8:1::1/32 any
Device(config-ipv6-acl)# deny tcp 2001:DB8:0300:0201::/32 eq telnet any
Device(config-ipv6-acl)# exit
Device(config)# interface Gigabitethernet 1/0/2
Device(config-if)# ipv6 traffic-filter ipv6acl out
Device(config-if)# end
```

Example: Creating and Applying an IPv6 ACL

The following example shows how to restrict HTTP access to certain hours during the day and log any activity outside of the permitted hours:

```
Device# configure terminal
Device(config)# time-range lunchtime
Device(config-time-range)# periodic weekdays 12:00 to 13:00
Device(config-time-range)# exit
Device(config)# ipv6 access-list OUTBOUND
Device(config-ipv6-acl)# permit tcp any any eq www time-range lunchtime
Device(config-ipv6-acl)# deny tcp any any eq www log-input
Device(config-ipv6-acl)# permit tcp 2001:DB8::/32 any
Device(config-ipv6-acl)# permit udp 2001:DB8::/32 any
Device(config-ipv6-acl)# end
```

Additional References for IPv6 Services—Standard Access Control Lists

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases

Related Topic	Document Title
Security commands	• Cisco IOS Security Command Reference: Commands A to C • Cisco IOS Security Command Reference: Commands D to L • Cisco IOS Security Command Reference: Commands M to R • Cisco IOS Security Command Reference: Commands S to Z
IPv6 Commands	Cisco IOS IPv6 Command Reference

Standards and RFCs

Standard/RFC	Title
RFC 2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IPv6 Services—Standard Access Control Lists

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to . An account on Cisco.com is not required.

Table 1: Feature Information for IPv6 Services—Standard Access Control Lists

Feature Name	Releases	Feature Information
IPv6 Services—Standard Access Control Lists	Cisco IOS XE Release 3.3SE	Access lists determine the type of traffic that is blocked or forwarded at device interfaces. Access control lists (ACLs) allow the filtering of inbound and outbound traffic based on source and destination addresses at interfaces. Standard IPv6 ACLs support traffic filtering based on IPv6 option headers and optional, upper-layer protocol type information. In Cisco IOS XE Release 3.3SE, this feature is supported on Cisco Catalyst 3850 Series Switches and Cisco 5700 Wireless LAN Controllers The following commands were introduced or modified: **ipv6 access-list**, **show ipv6 access-list**.