



## IPv6 ACL Chaining with a Common ACL

---

ACL Chaining, also known as Multi-Access Control List (ACL), allows you to split ACLs. This document describes how with the IPv6 ACL Chaining Support feature, you can explicitly split ACLs into common and user-specific ACLs and bind both ACLs to a target for traffic filtering on a device. In this way, the common ACLs in Ternary Content Addressable Memory (TCAM) are shared by multiple targets, thereby reducing the resource usage.

### Finding Feature Information

Your software release may not support all the features that are documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. The Feature Information Table at the end of this document provides information about the documented features and lists the releases in which each feature is supported.

### Contents

- [Hardware Compatibility Matrix for the Cisco cBR Series Routers, on page 1](#)
- [Information About IPv6 ACL Chaining with a Common ACL, on page 2](#)
- [How to Configure IPv6 ACL Chaining with a Common ACL, on page 3](#)
- [Configuration Examples for IPv6 ACL Chaining with a Common ACL, on page 4](#)
- [Additional References for IPv6 ACL Chaining with a Common ACL, on page 5](#)
- [Feature Information for IPv6 ACL Chaining with a Common ACL, on page 6](#)

## Hardware Compatibility Matrix for the Cisco cBR Series Routers



---

**Note** The hardware components that are introduced in a given Cisco IOS-XE Release are supported in all subsequent releases unless otherwise specified.

---

Table 1: Hardware Compatibility Matrix for the Cisco cBR Series Routers

| Cisco CMTS Platform                    | Processor Engine   | Interface Cards  |
|--|--|--|
| Cisco cBR-8 Converged Broadband Router | <p><b>Cisco IOS-XE Release 16.5.1 and Later Releases</b></p> <p>Cisco cBR-8 Supervisor:</p> <ul style="list-style-type: none"> <li>• PID—CBR-SUP-250G</li> <li>• PID—CBR-CCAP-SUP-160G</li> <li>• PID—CBR-CCAP-SUP-60G</li> <li>• PID—CBR-SUP-8X10G-PIC</li> </ul> | <p><b>Cisco IOS-XE Release 16.5.1 and Later Releases</b></p> <p>Cisco cBR-8 CCAP Line Cards:</p> <ul style="list-style-type: none"> <li>• PID—CBR-LC-8D30-16U30</li> <li>• PID—CBR-LC-8D31-16U30</li> <li>• PID—CBR-RF-PIC</li> <li>• PID—CBR-RF-PROT-PIC</li> <li>• PID—CBR-CCAP-LC-40G</li> <li>• PID—CBR-CCAP-LC-40G-R</li> </ul> <p>Cisco cBR-8 Downstream PHY Modules:</p> <ul style="list-style-type: none"> <li>• PID—CBR-D30-DS-MOD</li> <li>• PID—CBR-D31-DS-MOD</li> </ul> <p>Cisco cBR-8 Upstream PHY Modules:</p> <ul style="list-style-type: none"> <li>• PID—CBR-D30-US-MOD</li> <li>• PID—CBR-D31-US-MOD</li> </ul> |

## Information About IPv6 ACL Chaining with a Common ACL

### ACL Chaining Overview

The packet filter process supports only a single Access control list (ACL) to be applied per direction and per protocol on an interface. This leads to manageability and scalability issues if there are common ACL entries needed on many interfaces. Duplicate Access control entries (ACEs) are configured for all those interfaces, and any modification to the common ACEs needs to be performed for all ACLs.

A typical ACL on the edge box for an Internet Service Provider (ISP) has two sets of ACEs:

- Common ISP specific ACEs
- Customer/interface specific ACEs

The purpose of these address blocks is to deny access to ISP's protected infrastructure networks and anti-spoofing protection by allowing only customer source address blocks. This results in configuring unique ACL per interface and most of the ACEs being common across all ACLs on a device. ACL provisioning and modification is very cumbersome, hence, any changes to the ACE impacts every target.

## IPv6 ACL Chaining with a Common ACL

With IPv6 ACL Chaining, you can configure a traffic filter with the following:

- Common ACL
- Specific ACL
- Common and Specific ACL

Each Access control list (ACL) is matched in a sequence. For example, if you have specified both the ACLs - a common and a specific ACL, the packet is first matched against the common ACL; if a match is not found, it is then matched against the specific ACL.



**Note** Any IPv6 ACL may be configured on a traffic filter as a common or specific ACL. However, the same ACL cannot be specified on the same traffic filter as both common and specific.

## How to Configure IPv6 ACL Chaining with a Common ACL

### Before you begin

IPv6 ACL chaining is configured on an interface using an extension of the existing IPv6 traffic-filter command:  
**ipv6 traffic-filter** [**common** *common-acl*] [*specific-acl*] [ **in** | **out** ]



**Note** You may choose to configure either of the following:

- Only a common ACL. For example: **ipv6 traffic-filter common** *common-acl*
- Only a specific ACL. For example: **ipv6 traffic-filter** *common-acl*
- Both ACLs. For example: **ipv6 traffic-filter common** *common-acl specific-acl*

The `ipv6 traffic-filter` command is not additive. When you use the command, it replaces earlier instances of the command. For example, the command sequence: **ipv6 traffic-filter** [**common** *common-acl*] [*specific-acl*] **in** **ipv6 traffic-filter** [*specific-acl*] **in** binds a common ACL to the traffic filter, removes the common ACL and then binds a specific ACL.

## Configuring IPv6 ACL to an Interface

Perform this task to configure the interface to accept a common access control list (ACL) along with an interface-specific ACL:

### Procedure

|        | Command or Action                    | Purpose  |
|--------|--------------------------------------|--|
| Step 1 | <b>enable</b><br><br><b>Example:</b> | Enables privileged EXEC mode. Enter your password if prompted. |

|               | Command or Action   | Purpose   |
|---------------|---|---|
|               | Device> enable  |   |
| <b>Step 2</b> | <b>configure terminal</b><br><b>Example:</b><br>Device# configure terminal  | Enters global configuration mode.   |
| <b>Step 3</b> | <b>interface type number</b><br><b>Example:</b><br>Device(config)# interface<br>TenGigabitEthernet4/1/0                                   | Specifies the interface type and number, and enters interface configuration mode.       |
| <b>Step 4</b> | <b>ipv6 traffic filter {common-access-list-name {in   out}}</b><br><b>Example:</b><br>Device(config)# ipv6 traffic-filter<br>outbound out | Applies the specified IPv6 access list to the interface specified in the previous step. |
| <b>Step 5</b> | <b>end</b><br><b>Example:</b><br>Device(config-if)# end   | (Optional) Exits the configuration mode and returns to privileged EXEC mode.            |

## Configuration Examples for IPv6 ACL Chaining with a Common ACL

You may configure the following combinations in no particular order:

- A common ACL, for example: **ipv6 traffic-filter common common-acl in**
- A specific ACL, for example: **ipv6 traffic-filter specific-acl in**
- Both ACLs, for example: **ipv6 traffic-filter common common-acl specific-acl in**

### Example: Configuring an Interface to Accept a Common ACL

This example shows how to replace an access control list (ACL) configured on the interface without explicitly deleting the ACL:

```
interface TenGigabitEthernet4/1/0
ipv6 access-group common C_acl ACL1 in
end
replace interface acl ACL1 by ACL2
interface TenGigabitEthernet4/1/0
ipv6 access-group common C_acl ACL2 in
end
```

This example shows how to delete a common ACL from an interface. A common ACL cannot be replaced on interfaces without deleting it explicitly from the interface.

```
interface TenGigabitEthernet4/1/0
ipv6 access-group common C_acl1 ACL1 in
end
change the common acl to C_acl2
interface TenGigabitEthernet4/1/0
no ipv6 access-group common C_acl1 ACL1 in
end
interface TenGigabitEthernet4/1/0
ipv6 access-group common C_acl2 ACL1 in
end
```



**Note** When reconfiguring a common ACL, you must ensure that no other interface on the line card is attached to the common ACL.



**Note** If both common ACL and interface ACL are attached to an interface and only one of the above is reconfigured on the interface, then the other is removed automatically.

This example shows how to remove the interface ACL:

```
interface TenGigabitEthernet4/1/0
ipv6 access-group common C_acl1 ACL1 in
end
```

## Additional References for IPv6 ACL Chaining with a Common ACL

### Related Documents

| Related Topic             | Document Title   |
|---------------------------|--|
| IPv4 ACL Chaining Support | <a href="#">Security Configuration Guide: Access Control Lists, Cisco IOS XE Release 3S</a>  |
| Cisco IOS commands        | <a href="#">Cisco IOS Master Commands List, All Releases</a>   |
| Security commands         | <ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS Security Command Reference: Commands A to C</a></li> <li>• <a href="#">Cisco IOS Security Command Reference: Commands D to L</a></li> <li>• <a href="#">Cisco IOS Security Command Reference: Commands M to R</a></li> <li>• <a href="#">Cisco IOS Security Command Reference: Commands S to Z</a></li> </ul> |

**Technical Assistance**

| Description   | Link  |
|---|---|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/support">http://www.cisco.com/support</a> |

## Feature Information for IPv6 ACL Chaining with a Common ACL

Use Cisco Feature Navigator to find information about the platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to the [www.cisco.com/go/cfn](http://www.cisco.com/go/cfn) link. An account on the Cisco.com page is not required.



**Note** The following table lists the software release in which a given feature is introduced. Unless noted otherwise, subsequent releases of that software release train also support that feature.

**Table 2: Feature Information for IPv6 ACL Chaining with a Common ACL**

| Feature Name      | Releases                 | Feature Information  |
|-------------------|--------------------------|--|
| IPv6 access lists | Cisco IOS XE Fuji 16.7.1 | This feature was integrated into Cisco IOS XE Fuji 16.7.1 on the Cisco cBR Series Converged Broadband Routers. |