



MAC Access Control Lists

This chapter describes how to configure MAC access control lists (ACLs) on a Cisco router. It contains the following sections:

- [Finding Feature Information, on page 1](#)
- [Prerequisites for MAC Access Control Lists, on page 1](#)
- [Restrictions for MAC Access Control Lists, on page 1](#)
- [Information About MAC Access Control Lists, on page 2](#)
- [How to Configure MAC Access Control Lists, on page 2](#)
- [Configuration Examples for MAC Access Control Lists, on page 3](#)
- [Additional References for MAC Access Control Lists, on page 4](#)

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 <https://cfng.cisco.com/>. An account on Cisco.com is not required.

Prerequisites for MAC Access Control Lists

- You must be familiar with MAC addressing and non-IP protocols to configure MAC ACLs.

Restrictions for MAC Access Control Lists

- MAC ACL is supported only on EFP or TEFP.
- MAC ACL is not supported for IP packets.
- MAC ACL counters are not supported.
- MAC ACLs are not supported on port, routed interface, and BDI.

- ACL and QoS can be applied on the same EFP.
- Outbound MAC ACL is not supported.

Information About MAC Access Control Lists

MAC Access Control Lists

MAC ACLs are ACLs that filter traffic using information in the Layer 2 header of each packet. You can use ACLs to control which hosts can access different parts of a network or to decide which types of traffic are forwarded or blocked at the router interfaces. MAC ACL is supported on EFP and Cross-Connect.

How to Configure MAC Access Control Lists

Configuring ACL

To configure ACL, perform the steps below.

Procedure

Step 1 **enable**

Example:

```
Router> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Router# configure terminal
```

Enters global configuration mode.

Step 3 **mac access-list extended *name***

Example:

```
Router(config)# mac access-list ext macext2
```

Creates an extended MAC access control list (ACL) and define its access control entries (ACEs).

- *name*—Name of the ACL to which the entry belongs.

Step 4 **{permit | deny} {any | host *src-MAC-addr*} {any | host *dst-MAC-addr*}**

Example:

```
Router(config-ext-macl)# deny any any
```

Permits or denies Layer 2 traffic to be forwarded if the conditions are matched.

- **permit**—Permits Layer 2 traffic to be forwarded if the conditions are matched.
- **deny**—Denies Layer 2 traffic to be forwarded if the conditions are matched.
- **any**—Keyword to deny any source or destination MAC address.
- **host src-MAC-addr**—Defines a host MAC address. MAC address-based subnets are not allowed.
- **host dst-MAC-addr**—Defines a destination MAC address. MAC address-based subnets are not allowed.

Step 5 **end**

Example:

```
Router(config-ext-macl)# end
```

Returns to privileged EXEC mode.

Verifying MAC Access Control Lists

To verify the MAC ACL configuration, use the following **show** command.

- **show access-lists name**—Displays information about the named access list.

```
Router# show access-list macext4
```

```
Extended MAC access list macext4
 permit any host 0000.0000.0009
 permit any host 0000.0000.0010
 permit any host 0000.0000.0011
 permit any host 0000.0000.0012
```

Configuration Examples for MAC Access Control Lists

MAC ACL Configuration

Example: Allowing Specified Source or Destination MAC Addresses

```
(config)#mac access-list extended macext5
(config-ext-macl)#permit any host 0000.0000.0009
(config-ext-macl)#permit any host 0000.0000.0010
(config-ext-macl)#permit any host 0000.0000.0011
(config-ext-macl)#permit any host 0000.0000.0012
```

Example: Allowing any Source or Destination MAC Address

```
(config)#mac access-list extended macext9
(config-ext-macl)#permit any any
```

Additional References for MAC Access Control Lists

Related Documents

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

Standards and RFCs

Standard/RFC	Title
Standard	—

MIBs

MIB	MIBs Link
• CRCMB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

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>	http://www.cisco.com/cisco/web/support/index.html