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

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://cfnng.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 not supported on:
  - Trunk EFP or trunk port
  - Egress
  - Interface

- 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 cannot be applied on the same interface, EFP and bridge domain interface (BDI).
- Outbound MAC ACL is not supported on the Cisco RSP3 Module.
- MAC ACL does not deny broadcast packets on the EFP on the RSP3 module. To deny broadcast packets do any of the following:
  - Use storm control feature to restrict the broadcast packets.
  - Create a policy with the ACL (permit broadacst), and apply it to the interface with the 64K policer, to rate limit and allow only minimal amount of broadcast packets.

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.

Applying ACL on Cross-Connect

To apply ACL on Cross-Connect, perform the steps below.

Procedure

	Command or Action	Purpose
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	**interface gigabitethernet** *slot/subslot/port* **Example:** `Router(config)# interface gigabitEthernet 0/2/1`	Specifies an interface and enters interface configuration mode. • *slot/subslot/port*—The location of the interface.

	Command or Action	Purpose
Step 4	**service instance** *id* **ethernet** **Example:** `Router(config-if)# service instance 1120 ethernet`	Configures an Ethernet service instance on an interface and enters service instance configuration mode. • *id*—Specifies the EFP identifier, an integer from 1 to 4000.
Step 5	**description** *string* **Example:** `Router(config-if-srv)# description sBROBA 41CHE Shared VLAN highest priority`	Adds a description about an interface to help you remember its function. • *string*—Adds a description (up to 240 characters) for an interface.
Step 6	**encapsulation dot1q** *sp-vlan-id* **second-dot1q** { *ce-vlan-id* | **any**} **Example:** `Router(config-if-srv)# encapsulation dot1q 141 second-dot1q 120`	Enables stacked VLAN (802.1Q-in-Q) processing of customer VLAN traffic on an Ethernet subinterface. • *sp-vlan-id*—Virtual LAN identifier of the unique service-provider VLAN used in 802.1Q-in-Q encapsulation of Ethernet traffic from the VLANs of a customer. The valid values are from 1 to 4095. • *ce-vlan-id*—Virtual LAN identifier of a customer VLAN encapsulated with the service-provider VLAN ID specified by sp-vlan-id in stacked VLAN (802.1Q-in-Q) processing. The valid values are from 1 to 4095. This argument is the inner VLAN tag in 802.1Q-in-Q headers. • **any**—Configures stacked VLAN processing for all customer VLAN IDs encapsulated with the specified service-provider VLAN ID that are not specified in a separate encapsulation dot1q second-dot1q command on another subinterface.
Step 7	**rewrite ingress tag** {**pop** {**1** | **2**}} [**symmetric**] **Example:** `Router(config-if-srv)# rewrite ingress tag pop 2 symmetric`	Specifies the encapsulation adjustment that is to be performed on the frame ingress to the service instance. • **pop {1 | 2}**—One or two tags are removed from the packet. This command can be combined with a push (pop N and subsequent push vlan-id). • **symmetric**—(Optional) A rewrite operation is applied on both ingress and egress. The operation on egress is the inverse operation as ingress.

	Command or Action	Purpose
Step 8	**mac access-group** *access-list-name* **in** **Example:** `Router(config-if-srv)# mac access-group macext2 in`	To use a MAC access control list (ACL) to control inbound traffic on an Ethernet service instance. • *access-list-name*—Name of a MAC ACL to apply to an interface or subinterface (as specified by the mac access-list extended command). • **in**—Filters on inbound packets.
Step 9	**xconnect** *peer-router-id vcid* **encapsulation mpls** **Example:** `Router(config-if-srv)# xconnect 77.77.77.77 1120 encapsulation mpls`	Binds the attachment circuit to a pseudowire VC. The syntax for this command is the same as for all other Layer 2 transports. Enters cross-connect configuration mode. • *peer-router-id*—IP address of the remote provider edge (PE) peer router. • *vcid*—32-bit identifier to assign to the pseudowire.
Step 10	**mtu** *mtu-value* **Example:** `Router(config-if-xconn)# mtu 1500`	Specifies the MTU for the VC. • *mtu-value*—Specifies the value of the MTU.
Step 11	**exit** **Example:** `Router(config-if-xconn)# exit`	Exits cross-connect configuration mode.
Step 12	**service instance** *id* **ethernet** **Example:** `Router(config-if)# service instance 1000 ethernet`	Configures an Ethernet service instance on an interface and enters service instance configuration mode. • *id*—Specifies the EFP identifier, an integer from 1 to 4000.
Step 13	**encapsulation dot1q** *vlan-id* **Example:** `Router(config-if-srv)# encapsulation dot1q 141 second-dot1q 120`	To define the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance. • *vlan-id*—VLAN ID, integer in the range 1 to 4094.
Step 14	**mac access-group** *access-list-name* **in** **Example:** `Router(config-if-srv)# mac access-group macext2 in`	To use a MAC access control list (ACL) to control inbound traffic on an Ethernet service instance. • *access-list-name*—Name of a MAC ACL to apply to an interface or subinterface (as specified by the **mac access-list extended** command). • **in**—Filters on inbound packets.

	Command or Action	Purpose
Step 15	**bridge-domain** *bridge-id* **Example:** `Router(config-if-srv)# bridge-domain 1000`	Binds a service instance or a MAC tunnel to a bridge domain instance. • *bridge-id*—Numerical identifier for the bridge domain instance. The range is an integer from 1 to 4000.
Step 16	**end** **Example:** `Router(config-if-srv)# end`	Exits service instance mode and 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
• CISCO-AAA-SESSION-MIB	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
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html