Layer 2 Access Control Lists on EVCs

First Published: October 24, 2008
Last Updated: February 7, 2011

The ability to filter packets in a modular and scalable way is important for both network security and network management. Access Control Lists (ACLs) provide the capability to filter packets at a fine granularity. In Metro Ethernet networks, ACLs are directly applied on Ethernet virtual circuits (EVCs).

Layer 2 Access Control Lists on EVCs is a security feature that allows packet filtering based on MAC addresses. This module describes how to implement ACLs on EVCs.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 for Layer 2 Access Control Lists on EVCs" section on page 11.

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.

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for Layer 2 Access Control Lists on EVCs

- Knowledge of how service instances must be configured.
- Knowledge of extended MAC ACLs and how they must be configured.

Restrictions for Layer 2 Access Control Lists on EVCs

- A maximum of 16 access control entries (ACEs) are allowed for a given ACL.
- Only 256 different or unique Layer 2 ACLs can be configured on a line card. (More than 256 ACLs can be configured on a router.)
- Layer 2 ACLs function inbound only.
- Current Layer 2 ACLs provide Layer 3 filtering options in permit and deny rules. Options that are not relevant to service instances are ignored.

Information About Layer 2 Access Control Lists on EVCs

EVC

An EVC as defined by the Metro Ethernet Forum is a port-level point-to-point or multipoint-to-multipoint Layer 2 circuit. It is an end-to-end representation of a single instance of a Layer 2 service being offered by a provider to a customer. It embodies the different parameters on which the service is being offered. A service instance is the instantiation of an EVC on a given port on a given router.

Ethernet virtual connection services (EVCS) uses EVCs and service instances to provide Layer 2 switched Ethernet services. The EVC status can be used by a customer edge (CE) device either to find an alternative path in to the service provider network or, in some cases, to revert to a backup path over Ethernet or over another alternative service such as Frame Relay or ATM.

For information about the Metro Ethernet Forum standards, see the "Standards" section on page 10.

Relationship Between ACLs and Ethernet Infrastructure

The following points capture the relationship between ACLs and Ethernet Infrastructure (EI):

- ACLs can be directly applied on an EVC using the command-line interface (CLI). An ACL is applied to a service instance, which is the instantiation of an EVC on a given port.
- One ACL can be applied to more than one service instance at any time.
- One service instance can have one ACL at most applied to it at any time. If a Layer 2 ACL is applied to a service instance that already has a Layer 2 ACL, the new one replaces the old one.

- Only named ACLs can be applied to service instances. The command syntax ACLs is retained; the **mac access-list extended** command is used to create an ACL.
- The **show ethernet service instance** command can be used to provide details about ACLs on service instances.

How to Configure Layer 2 Access Control Lists on EVCs

Creating a Layer 2 ACL

Perform this task to create a Layer 2 ACL with a single ACE.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mac access-list extended** *name*
4. **permit** {{*src-mac mask* | **any**} {*dest-mac mask* | **any**} [*protocol* [**vlan** *vlan*] [**cos** *value*]]}

DETAILED STEPS

	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	**mac access-list extended** *name* **Example:** `Router(config)# mac access-list extended test-12-acl`	Defines an extended MAC ACL and enters mac access list control configuration mode.
Step 4	**permit** {{*src-mac mask* | **any**} {*dest-mac mask* | **any**} [*protocol* [**vlan** *vlan*] [*cos value*]]} **Example:** `Router(config-ext-macl)# permit 00aa.00bb.00cc 0.0.0 any`	Allows forwarding of Layer 2 traffic if the conditions are matched. Creates an ACE for the ACL.

Applying a Layer 2 ACL to a Service Instance

Perform this task to apply a Layer 2 ACL to a service instance. Note that packet filtering takes place only after the ACL has been created and applied to the service instance.

Prerequisites

Before applying an ACL to a service instance, you must create it using the **mac access-list extended** command. See the "Creating a Layer 2 ACL" section on page 3.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **service instance** *id* **ethernet**
5. **encapsulation dot1q** *vlan-id*
6. **mac access-group** *access-list-name* **in**

DETAILED STEPS

	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** *type number* **Example:** `Router(config)# interface gigabitethernet 1/0/0`	Specifies the type and location of the interface to configure, where: • *type*—Specifies the type of the interface. • *number*—Specifies the location of the interface.
Step 4	**service instance** *id* ethernet **Example:** `Router(config-if)# service instance 100 ethernet`	Configures an Ethernet service instance on an interface and enters Ethernet service configuration mode.

	Command or Action	Purpose
Step 5	**encapsulation dot1q** *vlan-id* **Example:** `Router(config-if-srv)# encapsulation dot1q 100`	Defines the matching criteria to be used in order to map ingress dot1q frames on an interface to the appropriate service instance.
Step 6	**mac access-group** *access-list-name* in **Example:** `Router(config-if-srv)# mac access-group test-12-acl in`	Applies a MAC ACL to control incoming traffic on the interface.

Configuring a Layer 2 ACL with ACEs on a Service Instance

Perform this task to configure the same ACL with three ACEs and stop all other traffic on a service instance.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mac access-list extended** *name*
4. **permit** {*src-mac mask* | **any**} {*dest-mac mask* | **any**}
5. **permit** {*src-mac mask* | **any**} {*dest-mac mask* | **any**}
6. **permit** {*src-mac mask* | **any**} {*dest-mac mask* | **any**}
7. **deny any any**
8. **exit**
9. **interface** *type number*
10. **service instance** *id* **ethernet**
11. **encapsulation dot1q** *vlan-id*
12. **mac access-group** *access-list-name* **in**

DETAILED STEPS

	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.

	Command or Action	Purpose
Step 3	**mac access-list extended** *name* **Example:** `Router(config)# mac access list extended test-12-acl`	Defines an extended MAC ACL and enters mac access control list configuration mode.
Step 4	**permit** {*src-mac mask* | **any**} {*dest-mac mask* | **any**} **Example:** `Router(config-ext-macl)# permit 00aa.bbcc.ddea 0.0.0 any`	Allows forwarding of Layer 2 traffic if the conditions are matched. This creates an ACE for the ACL.
Step 5	**permit** {*src-mac mask* | **any**} {*dest-mac mask* | **any**} **Example:** `Router(config-ext-macl)# permit 00aa.bbcc.ddeb 0.0.0 any`	Allows forwarding of Layer 2 traffic if the conditions are matched. This creates an ACE for the ACL.
Step 6	**permit** {*src-mac mask* | **any**} {*dest-mac mask*} | **any**} **Example:** `Router(config-ext-macl)# permit 00aa.bbcc.ddec 0.0.0 any`	Allows forwarding of Layer 2 traffic if the conditions are matched. This creates an ACE for the ACL.
Step 7	**deny any any** **Example:** `Router(config-ext-macl)# deny any any`	Prevents forwarding of Layer 2 traffic except for the allowed ACEs.
Step 8	**exit** **Example:** `Router(config-ext-macl)# exit`	Exits the current command mode and returns the CLI to global configuration mode.
Step 9	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 1/0/0`	Specifies the interface.
Step 10	**service instance** *id* **ethernet** **Example:** `Router(config-if)# service instance 200 ethernet`	Configures an Ethernet service instance on an interface and enters service instance configuration mode.

	Command or Action	Purpose
Step 11	**encapsulation dot1q** *vlan-id* **Example:** `Router(config-if-srv)# encapsulation dot1q 100`	Defines the matching criteria to be used to map ingress dot1q frames on an interface to the appropriate service instance.
Step 12	**mac access-group** *access-list-name* **in** **Example:** `Router(config-if-srv)# mac access-group test-12-acl in`	Applies a MAC ACL to control incoming traffic on the interface.

Verifying the Presence of a Layer 2 ACL on a Service Instance

Perform this task to verify that a Layer 2 ACL is present on an EVC. This verification task can be used after an ACL has been configured to confirm its presence.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **show ethernet service instance id** *id* **interface** *type number* **detail**

DETAILED STEPS

	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# show ethernet service instance id 100 interface gigabitethernet 3/0/1 detail`	Enters global configuration mode.
Step 3	**show ethernet service instance id** *id* **interface** *type number* detail **Example:** `Router# show ethernet service instance id 100 interface gigabitethernet 3/0/1 detail`	Displays detailed information about Ethernet customer service instances.

Configuration Examples for Layer 2 Access Control Lists on EVCs

- Example: Creating a Layer 2 ACL with ACEs
- Example: Applying a Layer 2 ACL to a Service Instance

Example: Creating a Layer 2 ACL with ACEs

The following example shows how to create a Layer 2 ACL called mac-11-acl with two permitted ACEs:

```
enable
configure terminal
mac access-list extended mac-11-acl
permit 00aa.00bb.00cc 1a11.0101.11c1 any
permit 00aa.00bb.00cc 1a11.0101.11c2 any
```

Example: Applying a Layer 2 ACL to a Service Instance

The following example shows how to apply a Layer 2 ACL called mac-20-acl to a service instance. The ACL has five permitted ACEs and all other traffic is not allowed.

```
enable
configure terminal
 mac access-list extended mac-20-acl
 permit 00aa.bbcc.adec 0.0.0 any
 permit 00aa.bbcc.bdec 0.0.0 any
 permit 00aa.bbcc.cdec 0.0.0 any
 permit 00aa.bbcc.edec 0.0.0 any
 permit 00aa.bbcc.fdec 0.0.0 any
 deny any any
 exit
interface gigabitethernet 10/0/0
 service instance 100 ethernet
 encapsulation dot1q 100
 mac access-group mac-20-acl in
```

Example: Applying a Layer 2 ACL to Three Service Instances on the Same Interface

The following example shows how to apply a Layer 2 ACL called mac-07-acl to three service instances on the same interface:

```
enable
configure terminal
mac access-list extended mac-07-acl
permit 00aa.bbcc.adec 0.0.0 any
permit 00aa.bbcc.bdec 0.0.0 any
permit 00aa.bbcc.cdec 0.0.0 any
deny any any
exit
interface gigabitethernet 10/0/0
service instance 100 ethernet
encapsulation dot1q 100
mac access-group mac-07-acl in
service instance 101 ethernet
encapsulation dot1q 101
mac access-group mac-07-acl in
```

```
service instance 102 ethernet
encapsulation dot1q 102
mac access-group mac-07-acl in
```

Example: Displaying the Details of a Layer 2 ACL on a Service Instance

The following sample output displays the details of a Layer 2 ACL called test-acl on a service instance.

```
Router# show ethernet service instance id 100 interface ethernet0/0 detail

Service Instance ID: 100
L2 ACL (inbound): test-acl
Associated Interface: Ethernet0/0
Associated EVC: test
L2protocol drop
CEVlans:
Interface Dot1q Tunnel Ethertype: 0x8100
State: Up
L2 ACL permit count: 10255
L2 ACL deny count: 53
```

Table 1 describes the significant fields in the output.

Table 1 show ethernet service instance Field Descriptions

Field	Description
Service Instance ID	Displays the service instance ID.
L2 ACL (inbound):	Displays the ACL name.
Associated Interface:	Displays the interface details of the service instance.
Associated EVC:	Displays the EVC with which the service instance is associated.
CEVlans:	Displays details of the associated VLAN ID.
State:	Displays whether the service instance is in an up or down state.
L2 ACL permit count:	Displays the number of packet frames allowed to pass on the service instance by the ACL.
L2 ACL deny count	Displays the number of packet frames not permitted to pass on the service instance by the ACL.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS Carrier Ethernet commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS Carrier Ethernet Command Reference*
Cisco IOS commands: master list of commands with complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS Master Commands List, All Releases*

Standards

Standard	Title
MEF 6.1	Metro Ethernet Services Definitions Phase 2 (PDF 6/08)
MEF 10.1	Ethernet Services Attributes Phase 2 (PDF 10/06)

MIBs

MIB	MIBs Link
• None	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this release.	—

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 Layer 2 Access Control Lists on EVCs

Table 2 lists the release history for this feature.

Use Cisco Feature Navigator to find information about 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 http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 2 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.

Table 2 Feature Information for Layer 2 Access Control Lists on EVCs

Feature Name	Releases	Feature Information
Layer 2 Access Control Lists on EVCs	12.2(33)SRD 15.0(1)S	The Layer 2 Access Control Lists on EVCs feature introduces ACLs on EVCs. • The following commands were introduced or modified: **interface, mac access-group in**, **mac access-list extended**, **show ethernet service instance**.