CHAPTER 3

Bridging Traffic

This chapter describes how clients and servers communicate through the ACE using either Layer 2 (L2) or Layer 3 (L3) in a VLAN configuration. When the client-side and server-side VLANs are on the same subnets, you can configure the ACE to bridge traffic on a single subnet mode.

When the client-side and server-side VLANs are on different subnets, you can configure the ACE to route the traffic. For more information, see Chapter 2, "Configuring Routes on the ACE."

In bridge mode, the ACE acts as a "bump in the wire" and is not a routed hop. No dynamic routing protocols are required.

When you configure a bridge group on an interface VLAN, the ACE automatically makes it a bridged interface. The ACE supports a maximum of two Layer 2 interface VLANs per bridge group.

Note The ACE does not allow shared VLAN configurations on Layer 2 interfaces.

Because L2 VLANs are not associated with an IP address, they require extended access control lists (ACLs) for controlling IP traffic. You can also optionally configure EtherType ACLs for the passing of non-IP traffic. For information on ACLs, see the *Cisco Application Control Engine Module Security Configuration Guide*.

To enable the bridge-group VLANs, you must configure a bridge-group virtual interface (BVI) that is associated with a corresponding bridge group. You must configure an IP address on the BVI. This address is used as a source IP address for traffic from the ACE, for example, Address Resolution Protocol (ARP) requests or management traffic. The ACE supports 4,094 BVIs per system.

Note The ACE supports a maximum of 8,192 interfaces per system that include VLANs, shared VLANs, and BVI interfaces.

The ACE does not perform MAC address learning on a bridged interface. Instead learning is performed by ARP. Bridge lookup is based on the bridge-group identifier and destination MAC address. A bridged interface automatically sends multicast and broadcast bridged traffic to the other interface of the bridge group.

ARP packets are always passed through an L2 interface after their verification and inspection. For information on configuring ARP on the ACE, see Chapter 4, "Configuring ARP." Multicast and broadcast packets from the incoming interface are flooded to the other L2 interface in the bridge group.

This chapter contains the following major sections:

- Bridge Mode Configuration Quick Start
- Configuring a Bridge-Group VLAN
- Configuring a Bridge-Group Virtual Interface
- Displaying Bridge Group or BVI Information
- Example of a Bridging Configuration

Bridge Mode Configuration Quick Start

Table 3-1 provides a quick overview of the steps required to configure a bridge group for the ACE. Each step includes the CLI command required to complete the task.

Table 3-1 Bridge Mode Configuration Quick Start

Task and Command Example

1. If you are operating in multiple context mode, observe the CLI prompt to verify that you are operating in the desired context. Change to the correct context if necessary.
`host1/Admin# changeto C1`
`host1/C1#`
The rest of the examples in this table use the Admin context unless otherwise specified. For details about creating contexts, see the *Cisco Application Control Engine Module Virtualization Configuration Guide*.

2. Access configuration mode by entering the **config** command.
`host1/Admin# config`
`Enter configuration commands, one per line. End with CNTL/Z`
`host1/Admin(config)#`

3. Create a VLAN for the bridge group and access interface configuration mode by using the **interface vlan** command. For example, enter:
`host1/Admin(config)# interface vlan 2`
`host1/Admin(config-if)#`

4. Assign the VLAN to the bridge group by using the **bridge-group** command. For example, enter: `host1/Admin(config-if)# bridge-group 15`

Table 3-1 Bridge Mode Configuration Quick Start (continued)

Task and Command Example

5. Assign an ACL to the VLAN to permit traffic by using the **access-group** command. You must configure an ACL on an interface where you want to permit traffic. Otherwise, the ACE denies all traffic on the interface. For more information on extended ACLs for IP traffic or EtherType ACLs for non-IP traffic, see the *Cisco Application Control Engine Module Security Configuration Guide*.
 	
The following example is an ACL that permits IP traffic:
 	
`access-list ACL1 line 5 extended permit ip any any`
 	
After you configure an ACL for the traffic, assign it to the VLAN. For example, to assign ACL1 for inbound traffic to the interface, enter:
 	
`host1/Admin(config-if)# access-group input ACL1`

6. Enable the VLAN by using the **no shutdown** command. For example, enter:
 	
`host1/Admin(config-if)# no shutdown`
`host1/Admin(config-if)# exit`

7. Configure a second VLAN for the bridge group. Repeat Steps 3 through 6.

8. Create a BVI for the bridge group and access interface configuration mode for the BVI by using the **interface bvi** command in configuration mode. For example, to create a BVI for bridge group 15, enter:
 	
`host1/Admin(config)# interface bvi 15`
`host1/Admin(config-if)#`

9. Assign an IP address to a BVI by using the **ip address** command. For example, to configure an IP address and mask for a BVI, enter: `host1/Admin(config-if)# ip address 10.0.0.81 255.0.0.0`
10. Enable a BVI by using the **no shutdown** command. For example, to enable a BVI, enter: `host1/Admin(config-if)# no shutdown`

Configuring a Bridge-Group VLAN

In bridge mode, you can configure two interface VLANs into a group and bridge packets between them. All interfaces are in one broadcast domain and packets from one VLAN are switched to the other VLAN. The ACE bridge mode supports only two L2 VLANs per bridge group. In this mode, L2 VLAN interfaces do not have configured IP addresses.

Before you create a bridge group, you must assign a VLAN to the context and access its mode to configure its attributes. Use the **interface vlan** command in configuration mode. The syntax of this command is as follows:

interface vlan *number*

The *number* argument is the VLAN number that you want to assign to the context. For example, enter:

```
host1/Admin(config)# interface vlan 2
```

To remove a VLAN, use the **no interface vlan** command. For example, enter:

```
host1/Admin(config)# no interface vlan 2
```

After you configure the VLAN, configure its attributes as described in the following topics:

- Configuring a Bridge Group to the VLAN
- Assigning an ACL to the Bridge-Group VLAN
- Enabling the Interface

Configuring a Bridge Group to the VLAN

When you configure a bridge group on the VLAN, the ACE automatically makes it bridged. To assign the VLAN to the bridge group, use the **bridge-group** command in interface configuration mode. The syntax of this command is as follows:

bridge-group *number*

The *number* argument is a number from 1 to 4094. For example, to assign bridge group 15 to the VLAN, enter:

```
host1/Admin(config-if)# bridge-group 15
```

To remove the bridge group from the VLAN, use the **no bridge-group** command. For example, enter:

```
host1/Admin(config-if)# no bridge-group
```

Assigning an ACL to the Bridge-Group VLAN

A bridge group VLAN supports extended ACLs for IP traffic and EtherType ACLs for non-IP traffic. The following is an example of an extended ACL that permits IP traffic:

```
host1/Admin(config)# access-list ACL1 line 5 extended permit ip any
any
```

When you configure access to an interface, the ACE applies it to all IP addresses configured on it.

For non-IP traffic, configure an EtherType ACL. EtherType ACLs support Ethernet V2 frames. You can configure the ACE to pass one or any of the following non-IP EtherTypes: Multiprotocol Label Switching (MPLS), Internet Protocol version 6 (IPv6), and bridge protocol data units (BDPUs).

You can permit or deny BPDUs. By default, all BPDUs are denied. The ACE receives trunk port (Cisco proprietary) BPDUs because ACE ports are trunk ports. Trunk BPDUs have VLAN information inside the payload, so the ACE modifies the payload with the outgoing VLAN if you permit BPDUs.

Note If you configure failover on the ACE, you must permit BPDUs on both interfaces with an EtherType ACL to avoid bridging loops.

The following example shows an EtherType ACL that permits BDPUs:

```
host1/Admin(config)#  access-list NONIP ethertype permit bdpu
```

Note The ACE does not forward minimum spanning tree (MST) BPDUs.

For more detailed information on extended or EtherType ACLs, see the *Cisco Application Control Engine Module Security Configuration Guide*.

After you configure an ACL for permitting traffic, assign it to the bridge-group VLAN. To apply an ACL to the inbound or outbound direction of a VLAN, use the **access-group** command in interface configuration mode. The syntax of this command is as follows:

access-group {**input** | **output**} *acl_name*

The options and arguments are as follows:

- **input**—Specifies the inbound direction of the interface to apply the ACL.
- **output**—Specifies the outbound direction of the interface to apply the ACL. This option is not allowed for EtherType ACLs.
- *acl_name*—Identifier of an existing ACL to apply to an interface

For example, to assign ACL1 for inbound traffic to the interface, enter:

```
host1/Admin(config-if)# access-group input ACL1
```

To assign ACL1 for outbound traffic to the interface, enter:

```
host1/Admin(config-if)# access-group output ACL1
```

To remove an ACL from an interface, use the **no access-group** command. For example, enter:

```
host1/Admin(config-if)# no access-group output ACL1
```

Enabling the Interface

When you create an interface, the interface is in the shutdown state until you enable it. To enable an interface for use, use the **no shutdown** command. For example, enter:

```
host1/Admin (config-if)# no shutdown
```

To disable the VLAN, use the **shutdown** command. For example, enter:

```
host1/Admin(config-if)# shutdown
```

After you enable the bridge-group VLAN, configure a BVI to bring it into operation.

Configuring a Bridge-Group Virtual Interface

To initiate traffic, such as ARP requests, from the ACE or for management traffic, a bridge group requires an interface with an IP address on the same subnet. This interface is the BVI.

A BVI is associated with a corresponding bridge group to routed interfaces within the router but acts as a routed interface that does not support bridging. The BVI is assigned with the number of the associated bridge group. Only one BVI is supported for each bridge group. The MAC address of the BVI is the same as the addresses of the associated bridge-group interfaces. You must enable the BVI and the associated bridge-group interfaces to forward traffic.

To use a BVI to terminate management traffic, apply a management policy to the Layer 2 interface from which the management traffic is expected. To apply this policy, configure the service policy on the bridge-group interface VLAN, and then configure the management IP address to the BVI.

This section contains the following topics:

Creating a Virtual Routed Interface for a Bridge Group

You can create a virtual routed interface for a bridge group by using the **interface bvi** command in configuration mode. The syntax of this command is as follows:

interface bvi *group_number*

The *group_number* argument is the bridge-group number configured on the Layer 2 VLAN interfaces.

For example, to create a BVI for bridge group 15, enter:

```
host1/Admin(config)# interface bvi 15
host1/Admin(config-if)#
```

To delete a BVI for bridge group 15, enter:

```
host1/Admin(config)# no interface bvi 15
```

Configuring a BVI IP Address

The ACE supports only one primary IP address with a maximum of four secondary addresses per interface. It treats the secondary addresses the same as a primary address and handles IP broadcasts and ARP requests for the subnet that assigned to the secondary address as well as the interface routes in the IP routing table.

The ACE accepts client, server, or remote access traffic on the primary and secondary addresses. When the destination for the control plane (CP)-originated packets is Layer 2 adjacent to either the primary subnet or one of the secondary subnets, the ACE uses the appropriate primary or secondary interface IP address for the destination subnet as the source IP address. For any destination that is not Layer 2 adjacent, the ACE uses the primary address as the source IP address. For packets destined to the secondary IP address, the ACE sends the response with the secondary IP address as the source address.

Note SSL probes use the primary IP address as the source address for all the destinations.

Observe the following requirements and restrictions when you assign an IP address to a BVI:

- You must configure a primary IP address before the interface can become active. The primary address must be active for a secondary address to be active.
- You can configure only one primary address per interface.
- You can configure a maximum of four secondary addresses per interface. The ACE has a system limit of 1,024 secondary addresses.
- When you configure access to an interface, the ACE applies all IP addresses configured the interface.

You can assign an IP address to a BVI by using the **ip address** command in interface configuration mode for the BVI. The syntax of this command is as follows:

ip address *ip_address mask* [**secondary**]

The arguments and option are as follows:

- *ip_address mask*—IP address and mask for the interface. Enter the IP address and subnet mask in dotted-decimal notation (for example, 192.168.1.1 255.255.255.0).

  If you do not include the **secondary** option, this address becomes the primary IP address. For the BVI to be active, you must configure a primary IP address for the interface.
- **secondary**—(Optional) Configures the address as a secondary IP address allowing multiple subnets under the same interface. You can configure a maximum of four secondary addresses per BVI. The ACE has a system limit of 1,024 secondary addresses.

Note The ACE has no counters specifically for traffic received or sent through secondary IP addresses. All counters are at the interface level or associated with the primary IP address.

For example, to configure an IP address and mask for a BVI, enter:

```
host1/Admin(config-if)# ip address 10.0.0.10 255.255.255.0
```

To assign a secondary IP address and mask 20.20.20.1 255.255.255.0 to a BVI, enter:

```
host1/Admin(config-if)# ip address 20.20.20.1 255.255.255.0 secondary
```

To delete the IP address from a BVI, enter:

```
host1/Admin(config-if)# no ip address
```

To remove a secondary IP address for the BVI, enter:

```
host1/Admin(config-if)# no ip address 20.20.20.1 255.255.255.0
secondary
```

Configuring an Alias IP Address

When you configure a redundant configuration with active and standby modules, you can configure a VLAN interface that has an IP address that is shared between the active and standby modules. To configure a shared address for the BVI, use the **alias** command in its interface configuration mode. The syntax of this command is as follows:

alias *ip_address mask* [**secondary**]

The arguments and option are as follows:

- *ip_address mask*—Alias IP address and subnet mask. Enter the IP address and subnet mask in dotted-decimal notation (for example, 192.168.1.1 255.255.255.0).
- **secondary**—(Optional) Configures the address as a secondary alias IP address. You can configure a maximum of four secondary addresses. The ACE has a system limit of 1,024 secondary alias addresses.

  The secondary alias address becomes active only when the corresponding secondary IP address on the same subnet is configured. If you remove the secondary IP address, the secondary alias address becomes inactive.

For example, to configure an IP address and mask for a BVI, enter:

```
host1/Admin(config-if)# alias 10.0.0.11 255.255.255.0
```

To configure a secondary alias IP address, enter:

```
host1/Admin(config-if)# alias 20.20.20.2 255.255.255.0 secondary
```

To delete the alias IP address from a BVI, enter:

```
host1/Admin(config-if)# no alias 10.0.0.11 255.255.255.0
```

To delete a secondary alias IP address, enter:

```
host1/Admin(config-if)# no alias 20.20.20.2 255.255.255.0 secondary
```

Configuring a Peer IP Address

When you configure redundancy, by default, configuration mode on the standby module is disabled and changes on an active module are automatically synchronized on the standby module. However, interface IP addresses on the active and standby modules must be unique. To ensure that the addresses on the interfaces are unique, the IP address of an interface on the active module is automatically synchronized on the standby module as the peer IP address.

To configure an IP address for the interface on the standby module, use the **peer ip address** command in interface configuration mode. The peer IP address on the active module is synchronized on the standby module as the interface IP address. The syntax of this command is as follows:

peer ip address *ip_address mask* [**secondary**]

The arguments and option are as follows:

- *ip_address mask*—IP address and mask for the peer ACE module. Enter the IP address and subnet mask in dotted-decimal notation (for example, 192.168.1.1 255.255.255.0).
- **secondary**—(Optional) Configures the address as a secondary peer IP address. You can configure a maximum of four secondary peer addresses. The ACE has a system limit of 1,024 secondary peer addresses.

Note When the destination for the control plane (CP)-originated packets is Layer 2 adjacent to either the primary subnet or one of the secondary subnets, the ACE always uses the appropriate primary or secondary interface IP address that belong to the destination subnet as the source IP address. For any destination that is not Layer 2 adjacent, the ACE uses the primary address as the source IP address. For packets destined to the secondary IP address, the ACE sends the response with the secondary IP address as the source address.

SSL probes always uses the primary IP address as the source address for all destinations.

You cannot configure secondary IP addresses on FT VLANs.

For example, to configure an IP address and mask for the peer module, enter:

```
host1/Admin(config-if)# peer ip address 10.0.0.12 255.255.255.0
```

To configure a secondary IP address and mask, enter:

```
host1/Admin(config-if)# peer ip address 20.20.20.3 255.255.255.0
secondary
```

To delete the IP address for the peer module, enter:

```
host1/Admin(config-if)# no peer ip address
```

To delete the secondary IP address for the peer ACE module, enter:

```
host1/Admin(config-if)# no peer ip address 20.20.20.3 255.255.255.0
secondary
```

Providing a BVI Description

You can provide a description for the BVI by using the **description** command in interface configuration mode. The syntax of this command is as follows:

description *text*

The *text* argument is a text string with a maximum of 240 alphanumeric characters including spaces.

For example, to provide a description for the BVI, enter:

```
host1/Admin(config-if)# description BVI for Bridge Group 15
```

To delete the description, enter:

```
host1/Admin(config-if)# no description
```

Enabling a BVI

You can enable a BVI by using the **no shutdown** command in interface configuration mode. The syntax of this command is as follows:

no shutdown

Note When you enable the interface, all of its configured primary and secondary addresses are enabled. You must configure a primary IP address before you can enable the interface. The ACE does not enable an interface with only secondary addresses. When you disable an interface, all of its configured primary and secondary addresses are disabled.

For example, to enable a BVI, enter:

```
host1/Admin(config-if)# no shutdown
```

To disable the BVI, enter:

```
host1/Admin(config-if)# shutdown
```

Displaying Bridge Group or BVI Information

You can display information about a bridge-group VLAN by using the **show interface vlan** command in Exec mode. For example, enter:

```
host1/Admin# show interface vlan 15
```

To display information about a BVI, use the **show interface bvi** command in Exec mode. For example, enter:

```
host1/Admin# show interface bvi 15
```

For information about the fields in the **show interface** command, see Table 1-1 in Chapter 1, "Configuring VLAN Interfaces."

Example of a Bridging Configuration

The following configuration is an example of how to configure bridging in the ACE.

```
login timeout 0

access-list ANYONE line 10 extended permit ip any any

probe tcp TCP

rserver host SERVER_01
  ip address 192.168.1.11
  inservice
rserver host SERVER_02
  ip address 192.168.1.12
  inservice
rserver host SERVER_03
  ip address 192.168.1.13
  inservice

serverfarm host REAL_SERVERS
  probe TCP
  rserver SERVER_11
    inservice
  rserver SERVER_12
    inservice
  rserver SERVER_13
    inservice

class-map match-all VIP-10
  2 match virtual-address 192.168.1.10 tcp eq www
class-map type management match-any REMOTE_ACCESS
  description remote-access-traffic-match
  2 match protocol telnet any
  3 match protocol ssh any
  4 match protocol icmp any

policy-map type management first-match REMOTE_MGT
  class REMOTE_ACCESS
    permit
```

```
policy-map type loadbalance first-match SLB_LOGIC
  class class-default
    serverfarm REAL_SERVERS
policy-map multi-match CLIENT_VIPS
  class VIP-10
    loadbalance vip inservice
    loadbalance policy SLB_LOGIC
    loadbalance vip icmp-reply active

interface vlan 201
  description Client vlan
  bridge-group 200
  access-group input ANYONE
  service-policy input REMOTE_MGT
  service-policy input CLIENT_VIPS
  no shutdown
interface vlan 202
  description Servers vlan
  bridge-group 200
  no shutdown
interface bvi 200
  description BVI interface for mgmt
  ip address 192.168.1.2 255.255.255.0
  no shutdown

ip route 0.0.0.0 0.0.0.0 192.168.1.1
```