CHAPTER 1

Configuring VLAN Interfaces

The Cisco Application Control Engine (ACE) module does not have any external physical interfaces to receive traffic from clients and servers. Instead, it uses internal VLAN interfaces. You assign VLANs from the supervisor engine to the ACE. After the VLANs are assigned to the ACE, you can configure the corresponding VLAN interfaces on the ACE as either routed or bridged. When you configure an IP address on an interface, the ACE automatically makes it a routed mode interface.

Similarly, when you configure a bridge group on an interface VLAN, the ACE automatically makes it a bridged interface. Then, you can associate a bridge-group virtual interface (BVI) with the bridge group. For more information on bridged groups and BVIs, see Chapter 3, "Bridging Traffic."

The ACE also supports shared VLANs, which are multiple interfaces in different contexts on the same VLAN within the same subnet. Only routed interfaces can share VLANs. Note that there is no routing across contexts even when shared VLANs are configured.

The ACE supports a maximum of 4093 VLANs per module and a maximum of 1024 shared VLANs per module.

Note The ACE supports a maximum of 8192 interfaces per module that include VLANs, shared VLANs, and BVI interfaces.

This chapter contains the following major sections:

Configuring VLANs Using Cisco IOS Software

To allow the ACE to receive traffic from the supervisor engine in the Catalyst 6500 series switch or Cisco 7600 series router, you must create VLAN groups on the supervisor engine and then assign the groups to the ACE. After the VLAN groups are assigned to the ACE, you can configure the VLAN interfaces on the ACE. By default, all VLANs are allocated to the Admin context on the ACE.

This section contains the following topics:

Creating VLAN Groups Using Cisco IOS Software

In Cisco IOS software, you can create one or more VLAN groups and then assign the groups to the ACE. For example, you can assign all the VLANs to one group, create an inside group and an outside group, or create a group for each customer.

You cannot assign the same VLAN to multiple groups; however, you can assign up to a maximum of 16 groups to an ACE. VLANs that you want to assign to multiple ACEs, for example, can reside in a separate group from VLANs that are unique to each ACE.

To assign VLANs to a group using Cisco IOS software on the supervisor engine, use the **svclc vlan-group** command. The syntax of this command is as follows:

svclc vlan-group *group_number vlan_range*

The arguments are as follows:

- *group_number*—Number of the VLAN group.
- *vlan_range*—One or more VLANs. The valid VLAN ranges are 2 to 1000 and 1025 to 4094 (VLANs 1001 to 1024 are reserved and cannot be used).

  VLANs are specified in one of the following ways:

  - A single number (*n*)
  - A range (*n-x*)

  Separate numbers or ranges by commas, as shown in this example:

  ```
  5,7-10,13,45-100
  ```

For example, to create three VLAN groups, 50 with a VLAN range of 55 to 57, 51 with a VLAN range of 75 to 86, and 52 with VLAN 100, enter:

```
Router(config)# svclc vlan-group 50 55-57
Router(config)# svclc vlan-group 51 70-85
Router(config)# svclc vlan-group 52 100
```

Assigning VLAN Groups to the ACE through Cisco IOS Software

The ACE cannot receive traffic from the supervisor engine unless you assign VLAN groups to it. To assign the VLAN groups to the ACE using Cisco IOS software on the supervisor engine, use the **svc module** command in configuration mode. The syntax of this command is as follows:

svc module *slot_number* **vlan-group** *group_number_range*

The arguments are as follows:

- *slot_number*—Slot number where the ACE resides. To display slot numbers and the modules in the chassis, use the **show module** command in Exec mode. The ACE appears as the Application Control Engine Module in the Card Type field.
- *group_number_range*—One or more group numbers that are identified in one of the following ways:

  - A single number (*n*)
  - A range (*n-x*)

  Separate numbers or ranges by commas, as shown in this example:

```
5,7-10
```

For example, to assign VLAN groups 50 and 52 to the ACE in slot 5, and VLAN groups 51 and 52 to the ACE in slot 8, enter:

```
Router(config)# svc module 5 vlan-group 50,52
Router(config)# svc module 8 vlan-group 51,52
```

To view the group configuration for the ACE and the associated VLANs, use the **show svclc vlan-group** command. For example, enter:

```
Router(config)# exit
Router# show svclc vlan-group
```

To view VLAN group numbers for all modules, use the **show svc module** command. For example, enter:

```
Router# show svc module
```

Note Enter the **show vlans** command in Exec mode from the Admin context to display the ACE VLANs that are downloaded from the supervisor engine.

Adding Switched Virtual Interfaces to the MSFC

A VLAN defined on the Multilayer Switch Feature Card (MSFC) is called a switched virtual interface (SVI). If you assign the VLAN used for the SVI to the ACE, then the MSFC routes between the ACE and other Layer 3 VLANs. By default, only one SVI can exist between the MSFC and the ACE. However, for multiple contexts, you may must configure multiple SVIs for unique VLANs on each context.

To add an SVI to the MSFC and configure it with a VLAN assigned to the ACE, perform the following steps:

Step 1 (Optional) If you need to add more than one SVI to the ACE, enter the following command:

```
Router(config)# svclc multiple-vlan-interfaces
```

Step 2 Add a VLAN interface to the MSFC. For example, to add VLAN 55, enter the following command:

```
Router(config)# interface vlan 55
```

Step 3 Set the IP address for this interface on the MSFC. For example, to set the address 10.1.1.1 255.255.255.0, enter the following command:

```
Router(config-if)# ip address 10.1.1.1 255.255.255.0
```

Step 4 Enable the interface. For example, enter the following command:

```
Router(config-if)# no shut
```

Note To monitor any VLAN that is associated with more than two trunk ports, physical ports, or trunk-physical ports on the supervisor engine, enable the autostate feature by using the **svclc autostate** command. When you associate at VLAN to these ports, autostate declares that the VLAN is up. When a VLAN state change occurs on the supervisor engine, autostate sends a notification to the ACE to bring the interface up or down.

To view this SVI configuration, use the **show interface vlan** command. For example, enter:

```
Router# show int vlan 55
```

Allocating VLANs to a User Context

By default, all VLANs assigned to the ACE are available at the Admin context. At the Admin context, you can assign a VLAN to a user context. VLANs can be shared across multiple contexts. However, the ACE supports only 1024 shared VLANs per system.

To view the VLANs assigned from the supervisor engine to the ACE, use the **show vlans** command in Exec mode from the Admin context.

If you try to configure a VLAN on a context that has not been allocated to it, the following error message is displayed:

```
Error: invalid input parameter <<<<<<<<<<<<
```

Note When a VLAN is shared in multiple contexts, the IP addresses across contexts must be unique and the interfaces must be on the same subnet. To classify traffic on multiple contexts, the same VLAN across contexts will have different MAC addresses. If you configure shared VLANs, no routing can occur across the contexts.

To assign VLAN interfaces to the context, access the context mode and use the **allocate-interface vlan** command in configuration mode. The syntax of this command is as follows:

allocate-interface vlan *vlan_number*

The *vlan_number* argument is the number of a VLAN or a range of VLANs assigned to the ACE.

Note The ACE allows you to assign a VLAN number to a context even if the VLAN has not been assigned from the supervisor engine to the ACE. You can configure the VLAN in the context, however the VLAN cannot receive traffic until it is assigned from the supervisor engine to the ACE.

For example, to assign VLAN 10 to context A, enter:

```
host1/Admin(config)# context A
host1/Admin(config-context)# allocate-interface vlan 10
```

To allocate an inclusive range of VLANs from VLAN 100 through VLAN 200 to a context, enter:

```
host1/Admin(config-context)# allocate-interface vlan 100-200
```

To remove a VLAN from a user context, use the **no allocate-interface vlan** command in context configuration mode. For example, enter:

```
host1/Admin(config)# context A
host1/Admin(config-context)# no allocate-interface vlan 10
```

Note You cannot deallocate a VLAN from a user context if the VLAN is currently in use on that context.

To remove a range of VLANs from a context, enter:

```
host1/Admin(config-context)# no allocate-interface vlan 100-200
```

Configuring a Bank of MAC Addresses for Shared VLANs

When contexts share a VLAN, the ACE assigns a different MAC address to the VLAN on each context. The MAC addresses reserved for shared VLANs are 0x001243dc6b00 to 0x001243dcaaff, inclusive. All ACE modules derive these addresses from a global pool of 16,000 MAC addresses. This pool is divided into 16 banks, each containing 1024 addresses. Each subnet can have 16 ACEs.

Each ACE supports 1024 shared VLANs, and uses only one bank of MAC addresses out of the pool. A shared MAC address is associated with a shared VLAN interface.

By default, the bank of MAC addresses that the ACE uses is randomly selected at boot time. However, if you configure two ACE modules in the same Layer 2 network and they are using shared VLANs, the ACEs may select the same address bank, which results in the use of the same MAC addresses. To avoid this conflict, you must configure the bank that the ACEs will use.

To configure a specific bank of MAC addresses for a local ACE or a peer ACE (in a redundant configuration), use the **shared-vlan-hostid** or the **peer shared-vlan-hostid** command, respectively, in configuration mode in the Admin context. The syntaxes of these commands are as follows:

shared-vlan-hostid *number*

peer shared-vlan-hostid *number*

The *number* argument indicates the bank of MAC addresses that the ACE uses. Enter a number from 1 to 16. Be sure to configure different bank numbers for multiple ACEs. For example, to configure bank 2 of MAC addresses for the local ACE and bank 3 for a peer ACE, enter:

```
host1/Admin(config)# shared-vlan-hostid 2
host1/Admin(config)# peer shared-vlan-hostid 3
```

To remove the configured bank of MAC addresses and allow the ACE to randomly select a bank, use the **no shared-vlan-hostid** command. For example, enter:

```
host1/Admin(config)# no shared-vlan-hostid
```

To remove the configured bank of MAC addresses from a peer ACE and allow it to randomly select a bank, use the **no peer shared-vlan-hostid** command. For example, enter:

```
host1/Admin(config)# no peer shared-vlan-hostid
```

Disabling the Egress MAC Lookup

Normally, the ACE performs a MAC address lookup when it receives a packet from the backplane and again when it forwards a packet out the egress interface. If you have multiple ACEs installed in a Catalyst 6500 Series Switch or in a Cisco Catalyst 7600 Router, you may experience lower performance than expected with very high rates of traffic. If you fail to achieve the advertised performance of the ACE, you can disable the egress MAC address lookup using the **hw-module optimize-lookup** command in configuration mode. The syntax of this command is as follows:

hw-module optimize-lookup

Note Do not use this command if you have intelligent modules with distributed forwarding cards (DFCs) installed in the Catalyst 6500 Series Switch or the Cisco Catalyst 7600 Router. Using this command with such modules will cause the Encoded Address Recognition Logic (EARL) units on these modules and on the Supervisor to become unsynchronized.

For example, to disable all egress MAC address lookups in the ACE, enter the following command:

```
Admin/host1(config)# hw-module optimize-lookup
```

To reenable egress MAC lookups, enter the following command:

```
Admin/host1(config)# no hw-module optimize-lookup
```

Configuring VLAN Interfaces on the ACE

You can configure a VLAN interface and access its mode to configure its attributes by using the **interface vlan** command in configuration mode for the context. The syntax of this command is as follows:

interface vlan *number*

The *number* argument is the VLAN number you want to assign to the interface. VLAN numbers are 2 to 4094. For example, to create VLAN 200, enter:

```
host1/Admin(config)# interface vlan 200
```

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

```
host1/Admin(config)# no interface vlan 200
```

Note For security reasons, the ACE does not allow pings from an interface on a VLAN on one side of the ACE through the module to an interface on a different VLAN on the other side of the module. For example, a host can ping the ACE address that is on the IP subnet using the same VLAN as the host, but cannot ping IP addresses configured on other VLANs on the ACE.

This section contains the following topics:

Note The ACE requires a route back to the client before it can forward a request to a server. If the route back is not present, the ACE cannot establish a flow and drops the client request. Make sure that you configure the appropriate routing to the client network on the ACE VLAN where the client traffic enters the ACE module.

Additional configurations and commands are available on a VLAN interface that are not documented in this chapter. These configurations are as follows:

- Remote network management—See the *Cisco Application Control Engine Module Administration Guide*.
- Default and static routes—See Chapter 2, "Configuring Routes on the ACE."
- Bridge parameters including the **interface bvi** command—See Chapter 3, "Bridging Traffic."
- Address Resolution Protocol (ARP)—See Chapter 4, "Configuring ARP."
- Dynamic Host Configuration Protocol (DHCP)—See Chapter 5, "Configuring the DHCP Relay."
- Policy and class maps, and SNMP management for VLANs, and fault-tolerant VLANs—See the *Cisco Application Control Engine Module Administration Guide*.
- Load balancing traffic including stealth firewall load balancing—See the *Cisco Application Control Engine Module Server Load-Balancing Guide*.
- ACLs, Network Address Translation (NAT), IP fragment reassembly, and IP normalization—See the *Cisco Application Control Engine Module Security Configuration Guide*.

Assigning IP Addresses to Interfaces for Routing Traffic

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 is 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 always use the primary IP address as the source address for all destinations.

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

- Assigning an IP address to a VLAN interface automatically makes it a routed mode interface.
- You must configure a primary IP address for the interface to allow a VLAN to become active. The primary address must be active before a secondary address can be active.
- You can configure only one primary address per VLAN.
- You can configure a maximum of four secondary addresses per VLAN. The ACE has a system limit of 1024 secondary addresses.
- In a single context, each interface address must be on a unique subnet and cannot overlap.
- In different contexts on a nonshared VLAN, the IP subnet can overlap an interface. However, on a shared VLAN, the IP address must be unique.
- Routed and bridged mode requires access control lists (ACLs) to allow traffic to pass. To apply an ACL to the inbound or outbound direction of an interface and make the ACL active, use the **access-group** command in interface configuration mode for the VLAN, as described in the "Applying an Access List to an Interface" section. For more information on configuring ACLs, see the *Cisco Application Control Engine Module Security Configuration Guide*.

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

When you configure remote network management access on an interface, the interface does not require an ACL. However, it does require a management class map and management policy map configuration. For information on configuring remote access to the ACE, see the *Cisco Application Control Engine Module Administration Guide*.

- You cannot configure secondary IP addresses on FT VLANs. When you configure a query interface to assess the health of the active FT group member, it uses the primary IP address.

To assign an IP address to a VLAN interface, use the **ip address** command in interface configuration mode. 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 VLAN 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. An interface can have only one primary IP address. To make the VLAN active, you must configure a primary IP address for the interface.

- **secondary**—(Optional) Configures the address as a secondary IP address that allows multiple subnets under the same VLAN. You can configure a maximum of four secondary addresses per VLAN. The ACE has a system limit of 1024 secondary addresses.

  The primary address must be active before the secondary address can be active.

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 assign the IP address and mask 192.168.1.1 255.255.255.0 to VLAN interface 200, enter:

```
host1/Admin(config)# interface vlan 200
host1/Admin(config-if)# ip address 192.168.1.1 255.255.255.0
```

If you make a mistake while entering this command, you can reenter the command with the correct information.

To assign a secondary IP address and mask 11.11.1.1 255.255.255.0 to VLAN interface 200, enter:

```
host1/Admin(config-if)# ip address 11.11.1.1 255.255.255.0 secondary
```

To remove the IP address for the VLAN, use the **no ip address** command. For example, enter:

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

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

```
host1/Admin(config-if)# no ip address 11.11.1.1 255.255.255.0
secondary
```

Disabling and Enabling Traffic on Interfaces

When you configure an interface, the interface is in the shutdown state until you enable it. If you disable or reenable the interface within a context, only that context interface is affected.

Note When you enable the interface, all of its configured primary and secondary addresses are enabled. You must configure a primary IP address to enable an 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.

To enable the interface, use the **no shutdown** command in interface configuration mode. For example, enter:

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

To disable a VLAN, use the **shutdown** command in interface configuration mode. The syntax of this command is as follows:

shutdown

For example, to disable VLAN 3, enter:

```
host1/Admin(config)# interface vlan 3
host1/Admin(config-if)# shutdown
```

Configuring the MTU for an Interface

The default maximum transmission unit (MTU) is a 1500-byte block for Ethernet interfaces. This value is sufficient for most applications, but you can pick a lower number if network conditions require this value (for example, to avoid fragmentation over IPSec tunnels) or a larger value (for example, for jumbo frames). Data that is larger than the MTU value is fragmented before being sent.

Caution If you configure a Layer 7 policy map and set the maximum transmit unit (MTU) of the ACE server-side VLAN lower than the client maximum segment size (MSS), ensure that the maximum value of the MSS that you set for the ACE using the **set tcp mss max** command is at least 40 bytes (size of the TCP header plus options) less than the MTU of the ACE server-side VLAN. Otherwise, the ACE may discard incoming packets from the server.

To specify the MTU for an interface, use the **mtu** command in interface configuration mode. This command allows you to set the data size that is sent on a connection. The syntax of this command is as follows:

mtu *bytes*

The *bytes* argument is the number of bytes in the MTU. Enter a number from 64 to 9216 bytes. The default is 1500.

For example, to specify the MTU data size of 1000 for an interface:

```
host1/Admin(config-if)# mtu 1000
```

To reset the MTU block size to 1500 bytes, use the **no mtu** command. For example, enter:

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

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 synchronized on the standby module as the peer IP address.

To configure the IP address for an interface on a 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, 192.168.1.20 255.255.255.0).
- **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 1024 secondary peer addresses.

Note The peer IP address must be unique across multiple contexts on a shared VLAN.

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 belongs 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 netmask of the peer module, enter:

```
host1/Admin(config-if)# peer ip address 192.168.1.20 255.255.255.0
```

To configure a secondary IP address and mask for the peer ACE module, enter:

```
host1/Admin(config-if)# peer ip address 11.11.1.2 255.255.255.0
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 11.11.1.2 255.255.255.0
secondary
```

Configuring an Alias IP Address

When you configure redundancy with active and standby modules, you can configure a VLAN interface that has an alias IP address that is shared between the active and standby modules. The alias IP address serves as a shared gateway for the two ACE modules in a redundant configuration.

Note You must configure redundancy (fault tolerance) on the ACE for the alias IP address to work. For more information on redundancy, see the *Cisco Application Control Engine Module Administration Guide*.

You cannot configure secondary IP addresses on FT VLANs.

The ACE also uses an alias IP address assigned to a VLAN to address a network device that you want to hide from the rest of the network. Typically, you assign alias IP addresses to VLANs with stealth firewalls so that the firewall remains invisible. An ACE uses the alias IP address configured on another ACE as the destination of the load-balancing process to direct flows through the firewalls. For details about configuring firewalls and firewall load balancing (FWLB) on the ACE, refer to the *Cisco Application Control Engine Module Server Load-Balancing Guide*.

To configure an alias IP address, use the **alias** command in interface configuration mode. The syntax of this command is as follows:

alias *ip_address netmask* [**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, 192.168.1.30 255.255.255.0).
- **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 1024 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 alias IP address, enter:

```
host1/Admin(config-if)# alias 192.168.1.30 255.255.255.0
```

To configure a secondary alias IP address, enter:

```
host1/Admin(config-if)# alias 11.11.1.3 255.255.255.0 secondary
```

To remove an alias IP address, enter:

```
host1/Admin(config-if)# no alias 192.168.1.30 255.255.255.0
```

To remove a secondary alias IP address, enter:

```
host1/Admin(config-if)# no alias 11.11.1.3 255.255.255.0 secondary
```

Autogenerating a MAC Address for a VLAN Interface

By default, the ACE does not allow traffic from one context to another context over a transparent firewall. The ACE assumes that VLANs in different contexts are in different Layer 2 domains, unless it is a shared VLAN. The ACE allocates the same MAC address to the VLANs.

When you are using a firewall service module (FWSM) to bridge traffic between two contexts on the ACE, you must assign two Layer 3 VLANs to the same bridge domain. To support this configuration, these VLAN interfaces require different MAC addresses.

To enable the autogeneration of a MAC address on a VLAN interface, use the **mac-address autogenerate** command in interface configuration mode. The syntax of this command is as follows:

mac-address autogenerate

For example, enter:

```
host1/Admin(config-if)# mac-address autogenerate
```

To disable MAC address autogeneration on the VLAN, use the **no mac address autogenerate** command. For example, enter:

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

Note When you use the **mac address autogenerate** command, the ACE assigns a MAC address from the bank of MAC address for shared VLANs. If you use the **no mac address autogenerate** command, the interface retains this address. To revert to a MAC address for an unshared VLAN, you must delete the interface and then add the interface again.

Enabling the Mac-Sticky Feature

The mac-sticky feature ensures that the ACE sends return traffic to the same upstream device through which the connection setup from the original client was received. When you enable this feature, the ACE uses the source MAC address from the first packet of a new connection to determine the device to send the return traffic. This guarantees that the ACE sends the return traffic for load-balanced connections to the same device originating the connection. By default, the ACE performs a route lookup to select the next hop to reach the client.

This feature is useful when the ACE receives traffic from Layer 2 and Layer 3 adjacent stateful devices, like firewalls and transparent caches, guaranteeing that it sends return traffic to the correct stateful device that sourced the connection

without any requirement for source NAT. For more information on firewall load balancing, see the *Cisco Application Control Engine Module Security Configuration Guide*.

To enable the mac-sticky feature for a VLAN interface, use the **mac-sticky enable** command in interface configuration mode. By default, the mac-sticky feature is disabled on the ACE. The syntax of this command is:

mac-sticky enable

Note You cannot use this command if you configure the **ip verify reverse-path** command. For information on the **ip verify reverse-path** command, see the*Cisco Application Control Engine Module Security Configuration Guide*.

For example, to enable the mac-sticky feature, enter:

```
host1/Admin(config-if)# mac-sticky enable
```

To disable the mac-sticky feature, use the **no mac-sticky enable** command. For example, enter:

```
host1/Admin(config-if)# no mac-sticky enable
```

Providing an Interface Description

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

description *text*

The *text* argument is the description for the interface. Enter an unquoted text string that contains a maximum of 240 alphanumeric characters including spaces.

For example, to provide the description of POLICY MAP 3 FOR INBOUND AND OUTBOUND TRAFFIC, enter:

```
host1/Admin(config-if)# description POLICY MAP3 FOR INBOUND AND
OUTBOUND TRAFFIC
```

To remove the description for the interface, use the **no description** command. For example, enter:

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

Configuring the UDP Booster Feature

When a network application requires very high UDP connection rates, configure the UDP booster feature. For detailed information concerning this feature and its configuration, see the *Cisco Application Control Engine Module Server Load-Balancing Guide*. To enable this feature, use the **udp** command in interface configuration mode. The syntax of this command is as follows:

udp {**ip-source-hash** | **ip-destination-hash**}

The keywords are as follows:

- **ip-source-hash**—Instructs the ACE to hash the source IP address of UDP packets that hit a source-hash VLAN interface prior to performing a connection match. Configure this keyword on a client-side interface.
- **ip-destination-hash**—Instructs the ACE to hash the destination IP address of UDP packets that hit a destination-hash VLAN interface prior to performing a connection match. Configure this keyword on a server-side interface.

For example, for a client-side interface, to enable the UDP hash forwarding on the source IP address of the UDP packets, enter:

```
host1/Admin(config)# interface vlan 100
host1/Admin(config-if)# udp ip-source-hash
```

To disable this feature, enter:

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

Assigning a Policy Map to an Interface

When you assign a policy map to a VLAN interface, the ACE can use the map to evaluate all network traffic on the interface. For more information on configuring policy maps, see the *Cisco Application Control Engine Module Administration Guide*.

You can apply one or more policy maps to a VLAN interface or globally to all VLAN interfaces in the same context. A policy map activated on an interface overwrites any specified global policy maps for overlapping classifications and actions.

You can assign multiple policy maps on an interface. However, the ACE allows only one policy map to be active on an interface at a given time. The order in which you configure the policy maps on the ACE is important.

To assign a policy map to an interface, use the **service-policy** command in interface configuration mode for an individual interface, or use the **service-policy** command in configuration mode for all interfaces in the same context.

The syntax of this command is as follows:

service-policy input *policy_name*

The keyword and argument are as follows:

- **input**—Specifies that the traffic policy is to be attached to the inbound direction of an interface. The traffic policy evaluates all traffic received by that interface.
- *policy_name*—Previously configured policy map that you want to apply to the interface.

For example, to specify a VLAN interface and apply multiple service policies to a VLAN, enter:

```
host1/Admin(config)# interface vlan 50
host1/Admin(config-if)# service-policy input L4_SLB_POLICY
```

For example, to globally apply multiple service policies to all of the VLANs associated with a context, enter:

```
host1/Admin(config)# service-policy input L4_SLB_POLICY
```

To remove a traffic policy from a VLAN interface, enter:

```
host1/Admin(config-if)# no service-policy input L4_SLB_POLICY
```

To globally remove a traffic policy from all VLANs associated with a context, enter:

```
host1/Admin(config)# no service-policy input L4_SLB_POLICY
```

Applying an Access List to an Interface

To allow the traffic to pass on an interface, you must apply ACLs to a VLAN interface. You can apply one ACL of each type (extended, ICMP, or EtherType) to both directions of the interface. For more information about ACLs and ACL directions, see the *Cisco Application Control Engine Module Security Configuration Guide*.

For connectionless protocols, you must apply the ACL to the source and destination interfaces if you want traffic to pass in both directions. For example, to allow Border Gateway Protocol (BGP) in an ACL in transparent mode, you must apply the ACL to both interfaces.

To apply an ACL to the inbound or outbound direction of an interface and make the ACL active, 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 t o apply the ACL.
- *acl_name*—Identifier of an existing ACL to apply to an interface.

For example, enter:

```
host1/Admin(config)# interface vlan100
host1/Admin(config-if)# access-group input INBOUND
```

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

```
host1/Admin(config-if)# no access-group input INBOUND
```

Displaying Interface Information

You can display information for the interfaces by using the **show interface** command. This section contains the following topics:

Displaying VLAN and BVI Information

You can use the **show interface** command in Exec mode to display the details, statistics, or IP information for all or a specified VLAN or BVI interface. The syntax of this command is as follows:

show interface [**bvi** *number* | **vlan** *number*]

The **bvi** | **vlan** *number* options display the information for the specified VLAN or bridge-group virtual interface number.

If you enter the **show interface** command with no options, the ACE displays all VLAN and BVI interfaces. For example, enter:

```
host1/Admin# show interface
```

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.

Table 1-1 describes the fields in the **show interface** command output.

Table 1-1 Field Descriptions for the show interface Command Output

Field	Description
VLAN_name/ *BVI_number* is	State of the specified VLAN or BVI (up, down, administratively up or down) and the reason for the transition to the state. **Note** The command output can include VLANs 1006 to 1011, which are reserved VLANs used by the ACE module and supervisor engine.
Hardware type is	Hardware type of the interface: either VLAN or BVI.
MAC address	MAC address of the system mapped to the IP address. Note that the BVI MAC address is the same address as an associated bridge-group VLAN address.
Mode	Mode associated with the VLAN or BVI. A bridge-group VLAN is displayed as transparent. A routed VLAN or BVI is displayed as routed. Otherwise, this field displays the value “unknown.”
FT status	Status of whether the interface is redundant.
Description	Description for the VLAN or BVI.
MTU	Configured MTU in bytes.
Last cleared	Last time that the VLAN or BVI was cleared.
Last Changed	Timestamp when the last change occurred.
No. of transitions	Number of transitions that the interface experienced since it was created.
Alias IP address	Configured alias IP address.
Peer IP address/netmask	Configured peer IP address and netmask.
Virtual MAC address	MAC address used by the alias IP address and VIP address when the interface is in the redundant active state (displayed only if the interface is in this state).

Table 1-1 Field Descriptions for the show interface Command Output (continued)

Field	Description
[Not] Assigned - Supervisor	Whether the VLAN or BVI is assigned from the supervisor engine and is up or down on the supervisor engine.
Previous State	Last three previous states including the timestamp and the reason for the up or down transitions.
# unicast packets input, # bytes	Total number of incoming unicast packets and number of bytes.
# multicast, # broadcast	Total number of incoming multicast and broadcast packets.
# input errors, # unknown, # ignored, # unicast RFP drops	Total number of errors for incoming packets, including numbers for packets that are unknown, ignored, and RFP drops.
# unicast packets output, # bytes	Total number of outgoing unicast packets and number of bytes.
# multicast, # broadcast	The total number of outgoing multicast and broadcast packets.
# output errors, # ignored	Number of errors for outgoing packets, including unknown packets.

Displaying VLAN and BVI Summary Statistics

You can use the **show ip interface brief** command in Exec mode to display a brief configuration and status summary of all interfaces or a specified BVI or a VLAN display. The syntax of this command is as follows:

show ip interface brief [**bvi** *number* | **vlan** *number*]

The **bvi | vlan** *number* options display the information for the specified VLAN or bridge-group virtual interface number.

If you enter the **show ip interface brief** command with no options, the ACE displays all VLAN and BVI interfaces. For example, enter:

```
host1/Admin# show ip interface brief
```

Table 1-2 describes the fields in the **show ip interface brief** command output.

Table 1-2 Field Descriptions for the show ip interface brief Command Output

Field	Description
Interface	VLAN or bridge-group virtual interface number.
IP Address	IP address and mask for the VLAN interface. If the interface is not assigned, the field displays unassigned.
Status	State of the interface: up, down, administratively up, administratively down.
Protocol	Status of the line protocol: either up or down.

Displaying the Interface Ethernet Out-of-Band Channel Information

You can display the Ethernet out-of-band channel (EOBC) information by using the **show interface eobc** command in Exec mode. This command is available in the Admin context only. For example, enter:

```
host1/Admin# show interface eobc
```

Table 1-3 describes the fields in the **show interface eobc** command output.

Table 1-3 Field Descriptions for the show interface eobc Command Output

Field	Description
Hardware type	Hardware type is EOBC.
MAC address	MAC address of the system mapped to the IP address.

Table 1-3 Field Descriptions for the show interface eobc Command Output (continued)

Field	Description
Description	Description for the VLAN.
MTU	MTU in bytes.
BW # bits/sec	Bits per second on the bus width.
IP address	Internal IP address.
# unicast packets input, # bytes	Total number of incoming unicast packets and number of bytes.
# input errors, # ignored	Number of errors for incoming packets, including numbers for packets that are ignored.
# unicast packets output, # bytes	Total number of outgoing unicast packets and number of bytes.
# output errors, # ignore	Number of errors for outgoing packets, including numbers for packets that are ignored.

Displaying the Internal Interface Manager Tables

You can display the internal interface manager tables and events by using the **show interface internal** command in Exec mode. The syntax of this command is as follows:

show interface internal {**event-history** {**dbg** | **mts**} |
iftable [*interface_name*] | **seciptable** | **vlantable** [*vlan_number*]}

The keywords and arguments are as follows:

- **event-history** {**dbg** | **mts**}—Displays the debug history (dbg) or message history (mts). This keyword is available in the Admin context only.
- **iftable** [*interface_name*]—Displays the master interface table. If you specify an interface name, the ACE displays the table information for that interface.
- **seciptable**—Displays the interface manager's (ifmgr) view of a logical interface and displays all the configured secondary IP addresses under an interface.

- **vlantable** [*vlan_number*]—Displays the VLAN table. If you specify an interface number, the ACE displays the table information for that interface.

Note The **show interface internal** command is used for debugging purposes. The output for this command is for use by trained Cisco personnel as an aid in debugging and troubleshooting the ACE. For information on the command syntax, see the *Cisco Application Control Engine Module Command Reference*.

For example, to display the interface internal debug event history starting with the most recent event, enter:

```
host1/Admin# show interface internal event-history dbg
```

To display the interface internal message event history starting with the most recent event, enter:

```
host1/Admin# show interface internal event-history mts
```

To display the master interface table, enter:

```
host1/Admin# show interface internal iftable
```

To display the master VLAN table, enter:

```
host1/Admin# show interface internal vlantable
```

Displaying ACE VLANs Downloaded from the Supervisor Engine

You can use the **show vlans** command in Exec mode for the Admin context to display the VLANs on the ACE downloaded from the supervisor engine. For example, enter:

```
host1/Admin# show vlans
Vlans configured on SUP for this module
    vlan192-193 vlan333
```

Displaying Private VLAN Information

The private VLAN feature on the Catalyst 6500 series switch or Cisco 7600 series router works with the ACE. The Cisco IOS PVLAN configuration populates the PVLAN mapping database on the ACE. See the documentation for the switch or router for detailed information.

To display the private VLANs on the ACE that are downloaded from the supervisor engine, use the **show pvlans** command in Exec mode. For example, enter:

```
host1/Admin# show pvlans
```

Table 1-4 describes the fields in the **show pvlans** command output.

Table 1-4 Field Descriptions for the show pvlans Command Output

Field	Description
Primary	VLAN number for the primary private VLAN.
Secondary	VLAN number for the secondary private VLAN.
Type	One of the three ways that the private VLAN uses VLANs: primary, isolated, or community.

Clearing Interface Statistics

You can clear the statistics displayed through the **show interface** command by using the **clear interface** command in Exec mode. The syntax of this command is as follows:

clear interface [**vlan** *number* | **bvi** *number*]

If you do not enter an option and argument, the statistics for all VLANs and BVIs are set to zero. The options and arguments are as follows:

- **vlan** *number*—Clears the statistics for the specified VLAN.
- **bvi** *number*—Clears the statistics for the specified BVI. Statistics are not collected for BVI interfaces. The packets are counted against the underlying bridged (Layer 2) interfaces.

For example to clear the statistics for VLAN 10, enter:

```
host1/Admin# clear interface vlan 10
```

Note If you configure redundancy, you must explicitly clear the statistics (hit counts) on both the active and the standby ACEs. If you clear the statistics on the active module only, the standby module statistics remain at the old values.