This chapter describes how to configure the VLAN interfaces on the Cisco 4700 Series Application Control Engine (ACE) appliance. 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 4, 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 4,093 VLANs per system and a maximum of 1,024 shared VLANs per system.

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

This chapter contains the following major sections:

- VLAN Interface Configuration Quick Start
- Configuring VLAN Interfaces on the ACE
- Allocating VLANs to a User Context
- Configuring a Bank of MAC Addresses for Shared VLANs
Table 2-1 provides a quick overview of the steps required to configure VLAN interfaces on the ACE. Each step includes the CLI command or a reference to the procedure required to complete the task. For a complete description of each feature and all the options associated with the CLI commands, see the sections following Table 2-1.

**Table 2-1  VLAN Interface Configuration Quick Start**

<table>
<thead>
<tr>
<th>Task and Command Example</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. If you are operating in multiple contexts, observe the CLI prompt to verify that you are operating in the desired context. If necessary, change to the correct context.</td>
<td></td>
</tr>
<tr>
<td>host1/Admin# <strong>changeto C1</strong> host1/C1#</td>
<td></td>
</tr>
<tr>
<td>The rest of the examples in this table use the C1 user context for illustration purposes, unless otherwise specified. For details on creating contexts, see the <em>Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide</em>.</td>
<td></td>
</tr>
<tr>
<td>2. Enter global configuration mode.</td>
<td></td>
</tr>
<tr>
<td>host1/Admin# <strong>config</strong> host1/Admin(config)#</td>
<td></td>
</tr>
<tr>
<td>3. If you have not already done so, configure Ethernet ports and specify VLAN trunking on the ACE. See Chapter 1, <em>Configuring Ethernet Interfaces</em>, for details.</td>
<td></td>
</tr>
<tr>
<td>4. Configure a VLAN interface and access its mode to configure its attributes. For example, to create VLAN 200, enter the following command:</td>
<td></td>
</tr>
<tr>
<td>host1/Admin(config)# <strong>interface vlan 200</strong></td>
<td></td>
</tr>
</tbody>
</table>
### Table 2-1  VLAN Interface Configuration Quick Start (continued)

<table>
<thead>
<tr>
<th>Task and Command Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>5. Assign an IP address to a VLAN interface for routing traffic. For example, to set the IP address of 192.168.1.1 255.255.255.0 for VLAN interface 200, enter the following command:</td>
</tr>
<tr>
<td>host1/Admin(config-if)# ip address 192.168.1.1 255.255.255.0</td>
</tr>
<tr>
<td>6. Enable the VLAN interface.</td>
</tr>
<tr>
<td>host1/Admin(config-if)# no shutdown</td>
</tr>
<tr>
<td>7. (Optional) Specify the MTU for a VLAN interface.</td>
</tr>
<tr>
<td>host1/Admin(config-if)# mtu 1000</td>
</tr>
<tr>
<td>8. (Optional) Configure the IP address for an interface on a standby ACE appliance.</td>
</tr>
<tr>
<td>host1/Admin(config-if)# peer ip address 11.0.0.81 255.0.0.0</td>
</tr>
<tr>
<td>9. (Optional) Enable reverse-path forwarding (RPF) based on a source MAC address for a VLAN interface.</td>
</tr>
<tr>
<td>host1/Admin(config-if)# mac-sticky enable</td>
</tr>
<tr>
<td>10. (Optional) Add a description about the interface to help you remember its function.</td>
</tr>
<tr>
<td>host1/Admin(config-if)# description FOR INBOUND AND OUTBOUND TRAFFIC</td>
</tr>
<tr>
<td>11. Assign a policy map to an interface. For example, to assign the SLB_OPTIMIZE_POLICY policy map for inbound traffic to the VLAN 3, enter the following command:</td>
</tr>
<tr>
<td>host1/Admin(config)# interface vlan 200</td>
</tr>
<tr>
<td>host1/Admin(config-if)# service-policy input SLB_OPTIMIZE_POLICY</td>
</tr>
<tr>
<td>12. Apply an ACL to the inbound or outbound direction of an interface and make the ACL active. For example, enter the following command:</td>
</tr>
<tr>
<td>host1/Admin(config-if)# access-group input INBOUND</td>
</tr>
<tr>
<td>host1/Admin(config-if)# exit</td>
</tr>
<tr>
<td>13. Assign VLAN interfaces to a specific context. For example, to assign VLAN 200 to context C1, enter the following command:</td>
</tr>
<tr>
<td>host1/Admin(config)# context C1</td>
</tr>
<tr>
<td>host1/C1(config-context)# allocate-interface vlan 200</td>
</tr>
</tbody>
</table>
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 for this command is as follows:

```
interface vlan number
```

The `number` argument is the VLAN number that you want to assign to the interface. Valid values are from 2 to 4094. By default, all devices are assigned to VLAN1, known as the default VLAN.

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
```

This section contains the following topics:

- Assigning IP Addresses to Interfaces for Routing Traffic
- Disabling and Enabling Traffic on Interfaces
- Configuring the MTU for an Interface
- Configuring a Peer IP Address
- Configuring an Alias IP Address
- Enabling the Mac-Sticky Feature
• Providing an Interface Description
• Assigning a Policy Map to an Interface
• Applying an Access List to an Interface

**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.

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

• Remote network management—See the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

• Allocate individual VLANs to a trunk link—See “Allocating an Ethernet Port or Port-Channel Interface to a VLAN Trunk” in Chapter 1, Configuring Ethernet Interfaces.

• IEEE 802.1Q Native VLAN for a trunk—See “Specifying the 802.1Q Native VLAN For a Trunk” in Chapter 1, Configuring Ethernet Interfaces.

• Access port to a specific VLAN—See “Configuring a VLAN Access Port” in Chapter 1, Configuring Ethernet Interfaces.

• Default and static routes—See Chapter 3, Configuring Routes on the ACE.

• Bridge parameters including the *interface bvi* command—See Chapter 4, Bridging Traffic.

• Address Resolution Protocol (ARP)—See Chapter 5, Configuring ARP.

• Dynamic Host Configuration Protocol (DHCP)—See Chapter 6, Configuring the DHCP Relay.

• Policy and class maps, and SNMP management for VLANs and fault-tolerant VLANs—See the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

• Load balancing traffic including stealth firewall load balancing—See the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*. 
Assigning IP Addresses to Interfaces for Routing Traffic

When you assign an IP address to a VLAN interface, the ACE automatically makes it a routed mode interface. To assign an IP address to a VLAN interface, use the `ip address` command in interface configuration mode. The syntax for this command is as follows:

```
  ip address ip_address mask
```

The `ip_address mask` arguments specify the 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).

**Note**
Secondary IP addresses are not supported on any ACE interfaces.

In a single context, each interface address must be on a unique subnet and cannot overlap. However, the IP subnet can overlap an interface in different contexts.

Across multiple contexts on a shared VLAN, the IP address must be unique. On a nonshared VLAN, the IP address can be the same.

For example, to assign the IP address and mask 192.168.1.1 255.255.255.0 to VLAN interface 200, enter the following command:

```
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, reenter the command with the correct information.
Note
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 4700 Series Application Control Engine Appliance Security Configuration Guide*.

To configure remote network management access on an interface, the interface does not require an ACL. However, it does require a class map and policy map configuration. For information on configuring remote access to the ACE, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

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

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

### 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.

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 for 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. Data that is larger than the MTU value is fragmented before being sent.

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 for 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 ACE appliance is disabled and changes on an active appliance are automatically synchronized on the standby ACE appliance. However, interface IP addresses on the active and standby ACE appliances must be unique. To ensure that the addresses on the interfaces are unique, the IP address of an interface on the active ACE appliance is synchronized on the standby ACE appliance as the peer IP address.

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

```
peer ip address ip_address mask
```
The `ip_address mask` arguments are the address and subnet mask for the peer ACE appliance. Enter the IP address and subnet mask in dotted-decimal notation (for example, 192.168.1.1 255.255.255.0).

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

For example, to configure an IP address and mask of the peer ACE appliance, enter:

```
host1/Admin(config-if)# peer ip address 11.0.0.81 255.0.0.0
```

To delete the IP address for the peer ACE appliance, enter:

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

### Configuring an Alias IP Address

When configuring a redundant configuration with active and standby appliances, you can configure a VLAN interface that has an alias IP address that floats between active and standby appliances. The alias IP address serves as a shared gateway for the two ACE appliances 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 4700 Series Application Control Engine Appliance Administration Guide*.

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 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*.

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

```
alias ip_address netmask
```
The `ip_address netmask` arguments specify the IP address and netmask 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).

For example, to configure an alias IP address, enter:

```
host1/Admin(config-if)# alias 192.168.12.15 255.255.255.0
```

To remove an alias IP address, enter:

```
host1/Admin(config-if)# no alias 192.168.12.15 255.255.255.0
```

### 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/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 4700 Series Application Control Engine Appliance 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 for 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 4700 Series Application Control Engine Appliance 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 for 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 for the interface, enter:

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

To remove the description for the interface, enter:

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

## 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 4700 Series Application Control Engine Appliance 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.
The **service-policy** command is available at both the interface configuration mode and at the configuration mode. Specifying a policy map in the interface configuration mode applies the policy map to a specific VLAN interface. Specifying a policy map in the configuration mode applies the policy to all of the VLAN interfaces associated with a context.

The syntax for this command is as follows:

```
service-policy input policy_name
```

The keywords, arguments, and options are as follows:

- **input**—Specifies that the traffic policy is to be attached to the inbound direction of a VLAN interface. The traffic policy evaluates all traffic received by that interface.

- **policy_name**—Previously configured policy map that you created using the **policy-map** command. The name can be a maximum of 64 alphanumeric characters.

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)# ip address 172.16.1.100 255.255.255.0
host1/Admin(config-if)# service-policy input L4_SLB_POLICY
host1/Admin(config-if)# service-policy input SLB_OPTIMIZE_POLICY
host1/Admin(config-if)# service-policy input HTTP_INSPECT_L4POLICY
```

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
host1/Admin(config)# service-policy input SLB_OPTIMIZE_POLICY
host1/Admin(config)# service-policy input HTTP_INSPECT_L4POLICY
```

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
```

You can remove a traffic policy either:
• Individually from the last VLAN interface on which you applied the service policy

• Globally from all VLAN interfaces in the same context

The ACE automatically resets the associated service policy statistics. The ACE performs this action to provide a new starting point for the service policy statistics the next time that you apply a traffic policy to a specific VLAN interface or globally to all VLAN interfaces in the same context.

Note the following when you create a service policy:

• Policy maps, applied globally in a context, are internally applied on all interfaces existing in the context.

• A policy activated on a VLAN interface overwrites any specified global policies for overlapping classification and actions.

• The ACE allows only one policy of a specific feature type to be activated on a given interface.

### 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 4700 Series Application Control Engine Appliance 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 for 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.
- **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
```
Allocating VLANs to a User Context

By default, all configured VLANs are available at 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

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.

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 for 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.

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 appliances 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 appliances 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 an ACE, use the `shared-vlan-hostid` command in configuration mode in the Admin context. The syntax for this command is as follows:

```
shared-vlan-hostid number
```

The `number` argument indicates the bank of MAC addresses that the ACE uses. Enter a number from 1 to 16.
For example, to configure bank 2 of MAC addresses, enter:

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

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
```

### Displaying VLAN or BVI Interface Information

You can display information for a VLAN or BVI interface by using the `show interface` command. This section contains the following topics:

- Displaying VLAN and BVI Information
- Displaying VLAN and BVI Summary Statistics
- Displaying the Internal Interface Manager Tables
- Clearing VLAN or BVI Interface Statistics

You can display information for an Ethernet data port, Ethernet management port, or a port-channel virtual interface by using the `show interface` command. See Chapter 1, Configuring Ethernet Interfaces, for details.

### 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 for this command is as follows:

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

The `bvi` or `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
```

Table 2-2 describes the fields in the `show interface` command output.
### Table 2-2 Field Descriptions for the show interface Command Output

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_name/ BVI_number</td>
<td>Status of the specified VLAN or BVI: either up or down.</td>
</tr>
<tr>
<td>Hardware type is</td>
<td>Hardware type of the interface: either VLAN or BVI.</td>
</tr>
<tr>
<td>MAC address</td>
<td>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.</td>
</tr>
<tr>
<td>Mode</td>
<td>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.”</td>
</tr>
<tr>
<td>FT status</td>
<td>Status of whether the interface is redundant.</td>
</tr>
<tr>
<td>Description</td>
<td>Description for the VLAN or BVI.</td>
</tr>
<tr>
<td>MTU</td>
<td>Configured MTU in bytes.</td>
</tr>
<tr>
<td>Last cleared</td>
<td>Last time that the VLAN or BVI was cleared.</td>
</tr>
<tr>
<td>Alias IP address</td>
<td>Configured alias IP address.</td>
</tr>
<tr>
<td>Peer IP address</td>
<td>Configured peer IP address.</td>
</tr>
<tr>
<td>Virtual MAC address</td>
<td>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).</td>
</tr>
<tr>
<td># unicast packets input,# bytes</td>
<td>Total number of incoming unicast packets and number of bytes.</td>
</tr>
<tr>
<td># multicast, # broadcast</td>
<td>Total number of incoming multicast and broadcast packets.</td>
</tr>
<tr>
<td># input errors, # unknown, # ignored, # unicast RFP drops</td>
<td>Total number of errors for incoming packets, including numbers for packets that are unknown, ignored, and RFP drops.</td>
</tr>
<tr>
<td># unicast packets output, # bytes</td>
<td>Total number of outgoing unicast packets and number of bytes.</td>
</tr>
</tbody>
</table>
### Displaying VLAN or BVI Interface Information

You can use the `show ip interface brief` command in Exec mode to display a brief configurational and status summary of all interfaces, or a specified BVI or a VLAN display. The syntax for 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 2-3 describes the fields in the `show ip interface brief` command output.

#### Table 2-3  Field Descriptions for the `show ip interface brief` Command Output

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>VLAN or bridge-group virtual interface number</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address and mask for the VLAN interface</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the specified VLAN or BVI: either up or down</td>
</tr>
<tr>
<td>Protocol</td>
<td>Status of the line protocol: either up or down</td>
</tr>
</tbody>
</table>

### Displaying VLAN and BVI Summary Statistics

You can use the `show ip interface brief` command in Exec mode to display a brief configurational and status summary of all interfaces, or a specified BVI or a VLAN display. The syntax for 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 2-3 describes the fields in the `show ip interface brief` command output.

#### Table 2-3  Field Descriptions for the `show ip interface brief` Command Output

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>VLAN or bridge-group virtual interface number</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address and mask for the VLAN interface</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the specified VLAN or BVI: either up or down</td>
</tr>
<tr>
<td>Protocol</td>
<td>Status of the line protocol: either up or down</td>
</tr>
</tbody>
</table>
Displaying the Internal Interface Manager Tables

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

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

The keywords and arguments are as follows:

- **event-history \{dbg | mts\}**—Displays the debug history (dbg) or message\n  history (mts). This keyword is available in the Admin context only.
- **iftable [interface_name]**—Displays the master interface table. If you specify\n  an interface name, the ACE displays the table information for that interface.
- **vlantable [vlan_number]**—Displays the VLAN table. If you specify an\n  interface number, the ACE displays the table information for that interface.

---

**Note**

The **show interface internal** command is used for debugging purposes. The\noutput for this command is for use by trained Cisco personnel as an aid in\ndiagnostic and troubleshooting the ACE. For information on the command syntax,\nsee the *Cisco 4700 Series Application Control Engine Appliance Command Reference*.

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

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

To display the interface internal message event history starting with the most\nrecent 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
```
Clearing VLAN or BVI Interface Statistics

You can clear the statistics displayed through the show interface command by using the clear interface command in Exec mode. The syntax for 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:

- **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 ACE appliance only, the standby ACE appliance statistics remain at the old values.
Clearing VLAN or BVI Interface Statistics