Cisco Application Control Engine Module
Routing and Bridging Configuration Guide

Software Version A2(3.0)
October 2009

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-20816-01
Preface vii
   Audience viii
   How to Use This Guide viii
   Related Documentation ix
   Symbols and Conventions xi
   Obtaining Documentation, Obtaining Support, and Security Guidelines xiii

CHAPTER 1
Configuring VLAN Interfaces 1-1
   Configuring VLANs Using Cisco IOS Software 1-2
      Creating VLAN Groups Using Cisco IOS Software 1-2
      Assigning VLAN Groups to the ACE through Cisco IOS Software 1-3
      Adding Switched Virtual Interfaces to the MSFC 1-4
   Allocating VLANs to a User Context 1-5
   Configuring a Bank of MAC Addresses for Shared VLANs 1-7
   Disabling the Egress MAC Lookup 1-8
   Configuring VLAN Interfaces on the ACE 1-9
      Assigning IP Addresses to Interfaces for Routing Traffic 1-10
      Disabling and Enabling Traffic on Interfaces 1-13
      Configuring the MTU for an Interface 1-14
      Configuring a Peer IP Address 1-15
      Configuring an Alias IP Address 1-16
      Autogenerating a MAC Address for a VLAN Interface 1-17
      Enabling the Mac-Sticky Feature 1-18
Contents

Providing an Interface Description 1-19
Configuring the UDP Booster Feature 1-20
Assigning a Policy Map to an Interface 1-21
Applying an Access List to an Interface 1-22

Displaying Interface Information 1-23
Displaying VLAN and BVI Information 1-23
Displaying VLAN and BVI Summary Statistics 1-25
Displaying the Interface Ethernet Out-of-Band Channel Information 1-26
Displaying the Internal Interface Manager Tables 1-27
Displaying ACE VLANs Downloaded from the Supervisor Engine 1-28
Displaying Private VLAN Information 1-28
Clearing Interface Statistics 1-29

CHAPTER 2

Configuring Routes on the ACE 2-1
Assigning an IP Address to Interfaces for a Routing Traffic 2-2
Configuring a Default or Static Route 2-3
Removing a Default or Static Route 2-4
Advertising a VLAN for RHI 2-4
Verifying Connectivity of a Remote Host or Server 2-5
Using Traceroute on the ACE-Configured IP Addresses 2-7
Displaying IP Route Information 2-8
Displaying FIB Table Information 2-13

CHAPTER 3

Bridging Traffic 3-1
Bridge Mode Configuration Quick Start 3-3
Configuring a Bridge-Group VLAN 3-5
 Configuring a Bridge Group to the VLAN 3-5
Assigning an ACL to the Bridge-Group VLAN 3-6
Enabling the Interface 3-7
Configuring a Bridge-Group Virtual Interface  3-8
   Creating a Virtual Routed Interface for a Bridge Group  3-8
   Configuring a BVI IP Address  3-9
   Configuring an Alias IP Address  3-11
   Configuring a Peer IP Address  3-12
   Providing a BVI Description  3-13
   Enabling a BVI  3-13
Displaying Bridge Group or BVI Information  3-14
Example of a Bridging Configuration  3-15

CHAPTER 4 Configuring ARP  4-1
   Adding a Static ARP Entry  4-2
   Enabling ARP Inspection  4-3
   Configuring the ARP Retry Attempts  4-4
   Configuring the ARP Retry Interval  4-5
   Configuring the ARP Request Interval  4-5
   Enabling the Learning of MAC Addresses  4-6
   Enabling Source MAC Validation  4-6
   Configuring the ARP Learned Interval  4-7
   Disabling the Replication of ARP Entries  4-8
   Specifying a Time Interval Between ARP Sync Messages  4-8
   Configuring the Rate Limit for Gratuitous ARP Packets  4-9
Displaying ARP Information  4-10
   Displaying IP Address-to-MAC Address Mapping  4-10
   Displaying ARP Statistics  4-11
   Displaying ARP Inspection Configuration  4-14
   Displaying ARP Timeout Values  4-15
Clearing ARP Learned Entries from the ARP Table  4-16
Clearing ARP Statistics  4-16

CHAPTER 5

Configuring the DHCP Relay  5-1
  DHCP Server and Client Overview  5-2
  DHCP Relay Configuration Quick Start  5-3
  Configuring the DHCP Relay Agent  5-4
    Enabling the DHCP Relay  5-4
    Specifying the DHCP Server IP Address  5-5
    Configuring a Relay Agent Information Reforwarding Policy  5-6
  Viewing DHCP Relay Configuration and Statistics  5-7

APPENDIX A

Addresses, Protocols, and Ports Reference  A-1
  IP Addresses and Subnet Masks  A-1
    Classes  A-2
    Private Networks  A-2
    Subnet Masks  A-3
      Determining the Subnet Mask  A-4
      Determining the Address to Use with the Subnet Mask  A-5
  Protocols and Applications  A-7
  TCP and UDP Ports  A-8
  ICMP Types  A-12

INDEX
Preface

This guide describes how to configure the routing and bridging features of the Cisco Application Control Engine (ACE) module for the Catalyst 6500 series switches or Cisco 7600 series router, hereinafter referred to as the switch or router, respectively.

This guide describes how to perform the following ACE configuration tasks:

- Configuring VLANs
- Configuring routing
- Configuring bridging
- Configuring Address Resolution Protocol (ARP)
- Configuring Dynamic Host Configuration Protocol (DHCP)

This preface contains the following major sections:

- Audience
- How to Use This Guide
- Related Documentation
- Symbols and Conventions
- Obtaining Documentation, Obtaining Support, and Security Guidelines
Audience

This guide is intended for the following trained and qualified service personnel who are responsible for configuring the ACE:

- Web master
- System administrator
- System operator

How to Use This Guide

This guide is organized as follows:

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1, Configuring VLAN Interfaces</td>
<td>Describes how to configure VLANs on the ACE.</td>
</tr>
<tr>
<td>Chapter 2, Configuring Routes on the ACE</td>
<td>Describes how to configure default and static routes.</td>
</tr>
<tr>
<td>Chapter 3, Bridging Traffic</td>
<td>Describes how to configure transparent (bridge) mode and a bridge-group virtual interface.</td>
</tr>
<tr>
<td>Chapter 4, Configuring ARP</td>
<td>Describes how to configure Address Resolution Protocol (ARP) parameters and enable ARP inspection.</td>
</tr>
<tr>
<td>Chapter 5, Configuring the DHCP Relay</td>
<td>Describes how to configure a Dynamic Host Configuration Protocol (DHCP) relay agent.</td>
</tr>
</tbody>
</table>
| Appendix A, Addresses, Protocols, and Ports Reference | Provides a reference for the following:  
  - IP addresses and subnet masks  
  - Protocols and applications  
  - TCP and UDP ports  
  - ICMP types |
## Related Documentation

In addition to this document, the ACE documentation set includes the following:

<table>
<thead>
<tr>
<th>Document Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Note for the Cisco Application Control Engine Module</td>
<td>Provides information about operating considerations, caveats, and command-line interface (CLI) commands for the ACE.</td>
</tr>
<tr>
<td>Cisco Application Control Engine Module Hardware Installation Note</td>
<td>Provides information for installing the ACE into the Catalyst 6500 series switch or Cisco 7600 series router.</td>
</tr>
<tr>
<td>Cisco Application Control Engine Module Getting Started Guide</td>
<td>Describes how to perform the initial setup and configuration tasks for the ACE.</td>
</tr>
</tbody>
</table>
| Cisco Application Control Engine Module Administration Guide | Describes how to perform the following administration tasks on the ACE:  
  • Setting up the ACE  
  • Establishing remote access  
  • Managing software licenses  
  • Configuring class maps and policy maps  
  • Managing the ACE software  
  • Configuring SNMP  
  • Configuring redundancy  
  • Configuring the XML interface  
  • Upgrading the ACE software |
<p>| Cisco Application Control Engine Module Virtualization Configuration Guide | Describes how to operate your ACE in a single context or in multiple contexts.                                                               |</p>
<table>
<thead>
<tr>
<th>Document Title</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Cisco Application Control Engine Module Server Load-Balancing Guide** | Describes how to configure the following server load-balancing tasks on the ACE:  
  - Real servers and server farms  
  - Class maps and policy maps to load balance traffic to real servers in server farms  
  - Server health monitoring (probes)  
  - Stickiness  
  - Firewall load balancing  
  - TCL scripts |
| **Cisco Application Control Engine Module Security Configuration Guide** | Describes how to configure the following ACE security features:  
  - Security access control lists (ACLs)  
  - User authentication and accounting using a Terminal Access Controller Access Control System Plus (TACACS+), Remote Authentication Dial-In User Service (RADIUS), or Lightweight Directory Access Protocol (LDAP) server  
  - Application protocol and HTTP deep packet inspection  
  - TCP/IP normalization and termination parameters  
  - Network Address Translation (NAT) |
| **Cisco Application Control Engine Module SSL Configuration Guide** | Describes how to configure the following Secure Sockets Layer (SSL) features on the ACE:  
  - SSL certificates and keys  
  - SSL initiation  
  - SSL termination  
  - End-to-end SSL |
Symbols and Conventions

This publication uses the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>boldface</strong> font</td>
<td>Commands, command options, and keywords are in <strong>boldface</strong>. Bold text also indicates a command in a paragraph.</td>
</tr>
<tr>
<td><em>italic</em> font</td>
<td>Arguments for which you supply values are in <em>italics</em>. Italic text also indicates the first occurrence of a new term, book title, emphasized text.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Elements in square brackets are optional.</td>
</tr>
<tr>
<td>Convention</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>{x</td>
<td>y</td>
</tr>
<tr>
<td>[x</td>
<td>y</td>
</tr>
<tr>
<td>string</td>
<td>A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.</td>
</tr>
<tr>
<td>screen font</td>
<td>Terminal sessions and information the system displays are in screen font.</td>
</tr>
<tr>
<td>boldface screen font</td>
<td>Information you must enter in a command line is in boldface screen font.</td>
</tr>
<tr>
<td>italic screen font</td>
<td>Arguments for which you supply values are in italic screen font.</td>
</tr>
<tr>
<td>^</td>
<td>The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.</td>
</tr>
<tr>
<td>&lt; &gt;</td>
<td>Nonprinting characters, such as passwords are in angle brackets.</td>
</tr>
</tbody>
</table>

Notes use the following conventions:

**Note**

Means reader take note. Notes contain helpful suggestions or references to material not covered in the publication.

Cautions use the following conventions:

**Caution**

Means reader be careful. In this situation, you might do something that could result in equipment damage or loss of data.

For additional information about CLI syntax formatting, see the *Cisco Application Control Engine Module Command Reference*. 
Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly What’s New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

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 4,093 VLANs per module and a maximum of 1,024 shared VLANs per module.

Note

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

This chapter contains the following major sections:

- Configuring VLANs Using Cisco IOS Software
- Allocating VLANs to a User Context
- Configuring a Bank of MAC Addresses for Shared VLANs
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
- Assigning VLAN Groups to the ACE through Cisco IOS Software
- Adding Switched Virtual Interfaces to the MSFC

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 (2 to 1000 and 1025 to 4094) 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:

\[ 5, 7-10, 13, 45-100 \]

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:

```plaintext
Router(config)# svc lc vlan-group 50 55-57
Router(config)# svc lc vlan-group 51 70-85
Router(config)# svc lc 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 need to 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:

1. **Optional** If you need to add more than one SVI to the ACE, enter the following command:
   
   ```
   Router(config)# svc multiple-vlan-interfaces
   ```

2. Add a VLAN interface to the MSFC. For example, to add VLAN 55, enter the following command:
   
   ```
   Router(config)# interface vlan 55
   ```
Chapter 1  Configuring VLAN Interfaces

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 <<<<<<<<<<<<<
```
Allocating VLANs to a User Context

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.

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
```

You cannot deallocate a VLAN from a user context if the VLAN is currently in use on that context.
Chapter 1  Configuring VLAN Interfaces

Configuring a Bank of MAC Addresses for Shared VLANs

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
```
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:

- 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
- Autogenerating a MAC Address for a VLAN Interface
- Enabling the Mac-Sticky Feature
- Providing an Interface Description
- Configuring the UDP Booster Feature
- 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 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.
Chapter 1   Configuring VLAN Interfaces

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 1,024 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 1,024 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 11.1.1.1 255.255.255.0 to VLAN interface 200, enter:

```
host1/Admin(config-if)# ip address 11.1.1.1 255.255.255.0 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 11.1.1.1 255.255.255.0 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:

```bash
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:

```bash
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:

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

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

```bash
host1/Admin(config-if)# no mtu
```
Chapter 1 Configuring VLAN Interfaces

Configuring VLAN Interfaces on the ACE

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 1,024 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 netmask` — 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 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 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 MAP 3 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 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
```
Chapter 1      Configuring VLAN Interfaces

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
- Displaying VLAN and BVI Summary Statistics
- Displaying the Interface Ethernet Out-of-Band Channel Information
- Displaying the Internal Interface Manager Tables
- Displaying ACE VLANs Downloaded from the Supervisor Engine
- Displaying Private VLAN Information

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:

```plaintext
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:

```plaintext
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>
<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</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>Assigned - Supervisor</td>
<td>Status of whether the VLAN or BVI is assigned from the supervisor engine and is up or down on the supervisor engine.</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>
</tbody>
</table>
Table 1-1  Field Descriptions for the show interface Command Output (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
<tr>
<td># multicast, # broadcast</td>
<td>The total number of outgoing multicast and broadcast packets.</td>
</tr>
<tr>
<td># output errors, # unknown</td>
<td>Number of errors for outgoing packets, including unknown packets.</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 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**

<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 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**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware type</td>
<td>Hardware type is EOBC.</td>
</tr>
<tr>
<td>MAC address</td>
<td>MAC address of the system mapped to the IP address.</td>
</tr>
<tr>
<td>Description</td>
<td>Description for the VLAN.</td>
</tr>
<tr>
<td>MTU</td>
<td>MTU in bytes.</td>
</tr>
<tr>
<td>BW # bits/sec</td>
<td>Bits per second on the bus width.</td>
</tr>
<tr>
<td>IP address</td>
<td>Internal IP address.</td>
</tr>
<tr>
<td># unicast packets input, # bytes</td>
<td>Total number of incoming unicast packets and number of bytes.</td>
</tr>
</tbody>
</table>
Displaying Interface Information

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td># input errors, # ignored</td>
<td>Number of errors for incoming packets, including numbers for packets that are ignored.</td>
</tr>
<tr>
<td># unicast packets output, # bytes</td>
<td>Total number of outgoing unicast packets and number of bytes.</td>
</tr>
<tr>
<td># output errors, # ignore</td>
<td>Number of errors for outgoing packets, including numbers for packets that are ignored.</td>
</tr>
</tbody>
</table>

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] | 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.
- `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>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary</td>
<td>VLAN number for the primary private VLAN.</td>
</tr>
<tr>
<td>Secondary</td>
<td>VLAN number for the secondary private VLAN.</td>
</tr>
<tr>
<td>Type</td>
<td>One of the three ways that the private VLAN uses VLANs: primary, isolated, or community.</td>
</tr>
</tbody>
</table>

**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.
This chapter describes how to configure a default or static route on the ACE and contains the following major sections:

- Assigning an IP Address to Interfaces for a Routing Traffic
- Configuring a Default or Static Route
- Removing a Default or Static Route
- Advertising a VLAN for RHI
- Verifying Connectivity of a Remote Host or Server
- Displaying IP Route Information
- Displaying FIB Table Information
Assigning an IP Address to Interfaces for a Routing Traffic

When you assign an IP address on an interface, its mode automatically becomes routed. 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
```

The `ip_address mask` arguments specify the IP address and mask for the VLAN interface.

For detailed information on configuring an IP address on an interface, see Chapter 1, “Configuring VLAN Interfaces.”

For example, to set the IP address of 192.168.1.1 255.255.255.0 for 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.
Configuring a Default or Static Route

Admin and user contexts do not support dynamic routing. You must use static routes for any networks to which the ACE is not directly connected; for example, you must use a static route when there is a router between a network and the ACE.

For traffic that originates on or is routed through the ACE and is destined for a nondirectly connected network, configure either a default route or static routes so that the ACE knows where to send the traffic. Traffic that originates on the ACE might include communications to a syslog server, Websense or N2H2 server, or AAA server.

The simplest option is to configure a default route to send all traffic to an upstream router. The default route identifies the router IP address where the ACE sends all IP packets for which it does not have a route.

Note

Routes that identify a specific destination address take precedence over the default route.

To set a default or static route, use the `ip route` command in configuration mode. The syntax of this command is as follows:

```
ip route dest_ip_prefix netmask gateway_ip_address
```

The keywords, arguments, and options are as follows:

- `dest_ip_prefix`—IP address for the route. Enter the address in dotted-decimal IP notation (for example, 192.168.20.1).
- `netmask`—Subnet mask for the route. Enter the subnet mask in dotted-decimal notation (for example, 255.255.255.0).
- `gateway_ip_address`—IP address of the gateway router (the next-hop address for this route). The gateway address must be in the same network as specified in the `ip address` command for a VLAN interface. For information on configuring the address, see the “Assigning an IP Address to Interfaces for a Routing Traffic” section.
Removing a Default or Static Route

You can remove a default or static IP route from the configuration by using the no form of the ip route command. For example, enter:

```
host1/Admin(config)# no ip route 192.168.42.0 255.255.255.0 192.168.1.5 1
```

Advertising a VLAN for RHI

To advertise a VLAN for route health injection (RHI) that is different from the VIP interface VLAN, use the ip route inject vlan command in interface configuration mode. By default, the ACE advertises the VLAN of the VIP interface for RHI.

Use this command when there is no directly shared VLAN between the ACE and the Catalyst 6500 series supervisor engine. This topology can occur when there is an intervening device, for example, a Cisco Firewall Services Module (FWSM), configured between the ACE and the supervisor engine.

Note

Management traffic coming into the ACE is not affected by the no normalization command, which does not support asymmetric routes. For information about normalization, see the Cisco Application Control Engine Module Security Configuration Guide.

For example, to configure a static route to send all traffic destined for 10.1.1.0/24 to the router (10.1.2.45), enter:

```
host1/Admin(config)# ip route 10.1.1.0 255.255.255.0 10.1.2.45
```

To configure a default route, set the IP address and the subnet mask for the route to 0.0.0.0. For example, if the ACE receives traffic that does not have a route and you want the ACE to send the traffic out the interface to the router at 192.168.4.8, enter:

```
host1/Admin(config)# ip route 0.0.0.0 0.0.0.0 192.168.4.8
```
Note

Be sure to configure this command on the VIP interface of the ACE.

The syntax of this command is as follows:

```
ip route inject vlan vlan_id
```

The `vlan_id` is the interface shared between the supervisor engine and the intervening device. Enter it as an integer from 2 to 4090.

For example, to advertise route 200 for RHI, enter:

```
host1/Admin(config-if)# ip route inject vlan 200
```

To restore the ACE default behavior of advertising the VIP interface VLAN for RHI, enter:

```
host1/Admin(config-if)# no ip route inject vlan 200
```

Verifying Connectivity of a Remote Host or Server

You can verify the connectivity of a remote host or server by using the `ping` command in Exec mode to send echo messages from the ACE.

The syntax of this command is as follows:

```
ping system_address
```

The `system_address` argument is the IP address of a remote host or server to ping. Enter an IP address in dotted-decimal notation (for example, 172.27.16.10).

The following example shows how to send a ping to a server located at IP address 192.168.219.140:

```
host1/Admin# ping 192.168.173.140
PING 192.168.173.140 with timeout = 2, count = 5, size = 100
Response from 192.168.173.140 : seq 1 time 1.213 ms
Response from 192.168.173.140 : seq 2 time 0.175 ms
Response from 192.168.173.140 : seq 3 time 0.210 ms
Response from 192.168.173.140 : seq 4 time 0.162 ms
Response from 11.1.11.4 : seq 5 time 0.214 ms
5 packet sent, 5 responses received, 0% packet loss
```

To abnormally terminate a ping session, press Ctrl-C.
The first ping may fail because the ARP table is not populated with the MAC address for the remote host or server.

The `ping` command provides additional options to verify the connectivity of a remote host or server. To specify these additional parameters, type `ping` at the CLI ACE prompt and press enter.

Table 2-1 summarizes the options and the defaults for the `ping` command.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target IP address</td>
<td>IP address or hostname of the destination node to ping.</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Repeat count</td>
<td>Number of ping packets to be sent to the destination address.</td>
<td>5 packets</td>
</tr>
<tr>
<td>Datagram size</td>
<td>Size of each ping packet in bytes.</td>
<td>100 bytes</td>
</tr>
<tr>
<td>Timeout in seconds</td>
<td>Timeout interval after which a ping request is considered a failure. The ping is not aborted and sends the next ping packet, if any.</td>
<td>2 seconds</td>
</tr>
<tr>
<td>Extended commands</td>
<td>Specifies whether a series of additional commands appear.</td>
<td>No</td>
</tr>
<tr>
<td>Source address or interface</td>
<td>Numeric IP address or the name of the source interface.</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Set DF bit in IP header</td>
<td>Path MTU Discovery strategy.</td>
<td>No</td>
</tr>
<tr>
<td>Time to Live</td>
<td>Value of the TTL field in the IP header that determines how long the ping packet exists before being discarded. The TTL value is reduced by one unit at each hop.</td>
<td>128</td>
</tr>
</tbody>
</table>

To trace the routes taken for a specified IP address, use the `traceroute` command in Exec mode.
The syntax of this command is as follows:

```
traceroute [ip_address [size packet]]
```

The arguments and option are as follows:

- `ip_address`—IP address for the route. Enter an IP address in dotted-decimal notation (for example, 172.27.16.10). This argument is optional if you do not include it with the command. You are prompted for an IP address.

- `size packet`—(Optional) Specifies the packet size. Enter a number from 40 to 452. The default is 40.

For example, to trace the IP address 192.168.173.140, enter:

```
host1/Admin# traceroute 192.168.173.140
traceroute to 192.168.173.140 (192.168.173.140), 30 hops max, 40 byte packets
1  192.86.215.2 (192.86.215.2)  0.558 ms  0.325 ms  0.297 ms
2  *   *   *
3  *   *   *
```

To terminate a traceroute session, press Ctrl-C.

### Using Traceroute on the ACE-Configured IP Addresses

You can use traceroute on ACE-configured IP addresses, however there are certain restrictions. When you use traceroute to a configured ACE IP interface:

- ICMP traceroute works when you configure a management policy to permit ICMP traffic, similar to the following example:

  ```
  class-map type management match-any remote-access
description remote-access-traffic-match
  match protocol icmp any
  ```

  **Note** Most traceroutes use the default protocol of UDP. Use a command line option to change traceroute to ICMP. For example, in Linux, use the `-I` option.

- UDP or TCP-based traceroute does not work. There is no method to permit UDP or TCP traffic to ephemeral ports going to the ACE.
When you use UDP, TCP, or ICMP-based traceroute to a host behind the ACE, it works as expected. However, the ACE does not appear in the traceroute as a hop. The ACE does not decrement the TTL of IP packets that it forwards.

When you use traceroute to a VIP address configured on the ACE, the ACE does not intercept traceroute packets sent to the configured VIP address. The ACE attempts to match the packet to the load-balance policies. If a protocol match occurs, the ACE sends the packet to the real server that responds to the traceroute accordingly.

## Displaying IP Route Information

To display IP routes on the ACE, use the `show ip route` command in Exec mode. For example, enter:

```
host1/Admin# show ip route
```

Table 2-2 describes the fields in the `show ip route` command output.

### Table 2-2 Field Description for the show ip route Command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>Destination address for the route.</td>
</tr>
<tr>
<td>Gateway</td>
<td>Gateway address for the route.</td>
</tr>
<tr>
<td>Interface</td>
<td>VLAN interface number for this entry.</td>
</tr>
</tbody>
</table>
| Flag | Flag to identify the route type and state, as identified by one of the following codes displayed above the output information:  
  - H indicates a host route.  
  - I indicates an interface route.  
  - S indicates a static route.  
  - N indicates a NAT route.  
  - A indicates that the route needs an ARP resolve.  
  - E indicates an ECMP route. |
To display the route summary for the current context, use the `show ip route summary` command. For example, enter:

```
host1/Admin# show ip route summary
```

Table 2-3 describes the fields in the `show ip route summary` command output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route Source</td>
<td>Source of the route. The possible value are as follows:</td>
</tr>
<tr>
<td></td>
<td>• Connected for a route to hosts that are connected to the same network.</td>
</tr>
<tr>
<td></td>
<td>• Static for a configured route.</td>
</tr>
<tr>
<td>Count</td>
<td>Number of routes that are connected or static.</td>
</tr>
<tr>
<td>Memory (bytes)</td>
<td>Memory consumed by the route entries.</td>
</tr>
</tbody>
</table>

To display IP traffic information, use the `show ip traffic` command in Exec mode. The syntax of this command is as follows:

```
show ip traffic
```

For example, enter:

```
host1/Admin# show ip traffic
```
Table 2-4 describes the fields in the `show ip traffic` command output.

**Table 2-4  Field Descriptions for the show ip traffic Command Output**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP Statistics</strong></td>
<td></td>
</tr>
<tr>
<td>Rcvd</td>
<td>Total number of packets received by the ACE, number of bytes received by the ACE, number of input errors, number of packets received by the ACE with no route, and number of packets received by the ACE that had an unknown protocol.</td>
</tr>
<tr>
<td>Frags</td>
<td>Number of fragments that the ACE reassembled, number of fragments that the ACE could not reassemble, number of packets that the ACE fragmented, and number of packets that the ACE could not fragment.</td>
</tr>
<tr>
<td>Bcast</td>
<td>Number of broadcast packets received and sent.</td>
</tr>
<tr>
<td>Mcast</td>
<td>Number of multicast packets received and sent.</td>
</tr>
<tr>
<td>Sent</td>
<td>Total packets sent, number of bytes sent, and number of packets sent with no route.</td>
</tr>
<tr>
<td>Drop</td>
<td>Number of packets discarded because they had no route and number of packets discarded.</td>
</tr>
</tbody>
</table>
### ICMP Statistics

ICMP Statistics reports statistics for the following ICMP messages received by the ACE:
- Redirects
- ICMP Unreachable
- ICMP Echo
- ICMP Echo Reply
- Mask Requests
- Mask Replies
- Quench
- Parameter
- Timestamp

ICMP Statistics reports statistics for the following ICMP messages sent by the ACE:
- Redirects
- ICMP Unreachable
- ICMP Echo
- ICMP Echo Reply
- Mask Requests
- Mask Replies
- Quench
- Parameter
- Timestamp
- Time Exceeded

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Recvd | Reports statistics for the following ICMP messages received by the ACE:  
- Redirects  
- ICMP Unreachable  
- ICMP Echo  
- ICMP Echo Reply  
- Mask Requests  
- Mask Replies  
- Quench  
- Parameter  
- Timestamp |
| Sent  | Reports statistics for the following ICMP messages sent by the ACE:  
- Redirects  
- ICMP Unreachable  
- ICMP Echo  
- ICMP Echo Reply  
- Mask Requests  
- Mask Replies  
- Quench  
- Parameter  
- Time Exceeded |
The show ip route internal command is used for debugging purposes. The output of 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.

### Table 2-4  Field Descriptions for the show ip traffic Command Output (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP Statistics</td>
<td></td>
</tr>
<tr>
<td>Rcvd</td>
<td>Total number of TCP segments and errors received by the ACE.</td>
</tr>
<tr>
<td>Sent</td>
<td>Total number of TCP segments sent by the ACE.</td>
</tr>
<tr>
<td>UDP Statistics</td>
<td></td>
</tr>
<tr>
<td>Rcvd</td>
<td>Total number of UDP segments, UDP errors, and segments with no port number received by the ACE.</td>
</tr>
<tr>
<td>Sent</td>
<td>Total number of UDP segments sent by the ACE.</td>
</tr>
<tr>
<td>ARP Statistics</td>
<td></td>
</tr>
<tr>
<td>Rcvd</td>
<td>Number of ARP packets, errors, requests, and responses received by the ACE.</td>
</tr>
<tr>
<td>Sent</td>
<td>Number of ARP packets, errors, requests, and responses sent by the ACE.</td>
</tr>
</tbody>
</table>
Displaying FIB Table Information

The forwarding information base (FIB) table contains information that the forwarding processors require to make IP forwarding decisions. This table is derived from the route and ARP tables. To display the FIB table for the context, use the `show ip fib` command. For example, enter:

`host1/Admin# show ip fib`

Table 2-5 describes the fields in the `show ip fib` command output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>Destination address for the route.</td>
</tr>
<tr>
<td>Interface</td>
<td>VLAN interface number for this entry.</td>
</tr>
<tr>
<td>EncapID</td>
<td>Encapsulation identifier.</td>
</tr>
<tr>
<td>Flag</td>
<td>Flag to identify the route type and state, as identified by one of the following codes displayed above the output information:</td>
</tr>
<tr>
<td></td>
<td>• H indicates a host route.</td>
</tr>
<tr>
<td></td>
<td>• I indicates interface route.</td>
</tr>
<tr>
<td></td>
<td>• S indicates a static route.</td>
</tr>
<tr>
<td></td>
<td>• N indicates a NAT route.</td>
</tr>
<tr>
<td></td>
<td>• A indicates that the route needs an ARP resolve.</td>
</tr>
<tr>
<td></td>
<td>• E indicates an ECMP route.</td>
</tr>
</tbody>
</table>

To display a summary of the FIB table for the context, use the `show ip fib summary` command. For example, enter:

`host1/Admin# show ip fib summary`
Table 2-6 describes the fields in the `show ip fib summary` command output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resolved routes</td>
<td>Number of prefixes programmed in mtrie.</td>
</tr>
<tr>
<td>Leaves, bytes</td>
<td>Number of mtrie leaf nodes allocated and memory consumed in bytes.</td>
</tr>
<tr>
<td>Nodes, bytes</td>
<td>Number of mtrie internal nodes allocated and memory consumed in bytes.</td>
</tr>
<tr>
<td>ecmps, bytes</td>
<td>Number of ECMP nodes allocated and memory consumed in bytes.</td>
</tr>
</tbody>
</table>

The `show ip fib` command is used for debugging purposes. The output of 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*. 
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.

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**

<table>
<thead>
<tr>
<th>Task and Command Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

```
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.

<table>
<thead>
<tr>
<th>Task and Command Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Access configuration mode by entering the <strong>config</strong> command.</td>
</tr>
</tbody>
</table>

```
host1/Admin# config
Enter configuration commands, one per line. End with CNTL/Z
host1/Admin(config)#
```

<table>
<thead>
<tr>
<th>Task and Command Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>3. Create a VLAN for the bridge group and access interface configuration mode by using the <strong>interface vlan</strong> command. For example, enter:</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Task and Command Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>4. Assign the VLAN to the bridge group by using the <strong>bridge-group</strong> command. For example, enter:</td>
</tr>
</tbody>
</table>

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

```plaintext
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:

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

6. Enable the VLAN by using the `no shutdown` command. For example, enter:

```plaintext
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:

```plaintext
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:

```plaintext
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:

```plaintext
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 \textit{number} argument is a number from 1 to 4094. For example, to assign bridge group 15 to the VLAN, enter:

\begin{verbatim}
host1/Admin(config-if)# bridge-group 15
\end{verbatim}

To remove the bridge group from the VLAN, use the \texttt{no bridge-group} command. For example, enter:

\begin{verbatim}
host1/Admin(config-if)# no bridge-group
\end{verbatim}

### 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:

\begin{verbatim}
host1/Admin(config)# access-list ACL1 line 5 extended permit ip any any
\end{verbatim}

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.

\begin{verbatim}
host1/Admin(config)# access-list NONIP ethertype permit bdpu
\end{verbatim}

\textbf{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:

\begin{verbatim}
host1/Admin(config)# access-list NONIP ethertype permit bdpu
\end{verbatim}

\textbf{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.
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
- Configuring a BVI IP Address
- Configuring an Alias IP Address
- Configuring a Peer IP Address
- Providing a BVI Description
- Enabling a BVI

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:

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

To disable the BVI, enter:

```plaintext
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:

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

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

```plaintext
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.

```bash
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
```
Example of a Bridging Configuration

```plaintext
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
```
This chapter describes how the Address Resolution Protocol (ARP) on the ACE can manage and learn the mapping of IP to Media Access Control (MAC) information to forward and transmit packets. The ACE creates an ARP cache entry when it receives an ARP packet or you configure an IP address on the ACE (for example, an IP address for a real server, gateway, or an interface VLAN).

You can also configure static ARP entries for IP to Media Access Control (MAC) translations and ARP inspection to prevent ARP spoofing. ARP inspection ensures that an attacker cannot send an ARP response with the attacker MAC address if the correct MAC address and the associated IP address are in the static ARP table.

This chapter describes how to configure ARP parameters and enable ARP inspection, and contains the following major sections:

- Adding a Static ARP Entry
- Enabling ARP Inspection
- Configuring the ARP Retry Attempts
- Configuring the ARP Retry Interval
- Configuring the ARP Request Interval
- Enabling the Learning of MAC Addresses
- Enabling Source MAC Validation
- Configuring the ARP Learned Interval
- Disabling the Replication of ARP Entries
- Specifying a Time Interval Between ARP Sync Messages
Adding a Static ARP Entry

To add a static ARP entry in the ARP table, use the `arp` command in configuration mode or in interface configuration mode. You can create a static ARP entry at the context level. For bridged interfaces, you must configure static ARP entries in interface configuration mode.

Note

When you enable ARP inspection, the ACE compares ARP packets with static ARP entries in the ARP table to determine what action to take. For more information, see the “Enabling ARP Inspection” section.

The syntax of this command is as follows:

```
arp ip_address mac_address
```

The arguments are as follows:

- `ip_address`—IP address for an ARP table entry. Enter the IP address in dotted-decimal notation (for example, 172.16.56.76).
- `mac_address`—Hardware MAC address for the ARP table entry. Enter the MAC address in dotted-hexadecimal notation (for example, 00.60.97.d5.26.ab).

For example, to allow ARP responses from the router at 10.1.1.1 with the MAC address 00.02.9a.3b.94.d9, enter the following command:

```
host1/Admin(config)# arp 10.1.1.1 00.02.9a.3b.94.d9
```

To remove a static ARP entry, use the `no arp` command. For example, enter:

```
host1/Admin(config)# no arp 10.1.1.1 00.02.9a.3b.94.d9
```
Enabling ARP Inspection

ARP inspection prevents malicious users from impersonating other hosts or routers, known as ARP spoofing. ARP spoofing can enable a “man-in-the-middle” attack. For example, a host sends an ARP request to the gateway router. The gateway router responds with the gateway router MAC address.

However, the attacker sends another ARP response to the host with the attacker MAC address instead of the router MAC address. The attacker can now intercept all the host traffic before forwarding it on to the router. ARP inspection ensures that an attacker cannot send an ARP response with the attacker MAC address if the correct MAC address and the associated IP address are in the static ARP table.

ARP inspection operates only on ingress bridged interfaces. By default, ARP inspection is disabled on all interfaces, allowing all ARP packets through the ACE. When you enable ARP inspection, the ACE uses the IP address and interface ID (ifID) of an incoming ARP packet as an index into the ARP table. The ACE then compares the MAC address of the ARP packet with the MAC address in the indexed static ARP entry in the ARP table and takes the following actions:

- If the IP address, source ifID, and MAC address match a static ARP entry, the inspection succeeds and the ACE allows the packet to pass.
- If the IP address and interface of the incoming ARP packet match a static ARP entry, but the MAC address of the packet does not match the MAC address that you configured in that static ARP entry, ARP inspection fails, the ACE drops the packet, and it increments the Inspect Failed counter regardless of whether the flood or no-flood option is configured.
- If the ARP packet does not match any static entries in the ARP table or there are no static entries in the table, then you can set the ACE to either forward the packet out all interfaces (flood) or to drop the packet (no-flood). In this case, the source IP address to MAC address mapping is new to the ACE. If you enter the flood option, the ACE creates a new ARP entry and marks it as LEARNED. If you enter the no-flood option, the ACE drops the ARP packet.

To enable ARP inspection, use the arp inspection enable command in configuration mode. The syntax of this command is as follows:

arp inspection enable [flood | no-flood]
The options are as follows:

- **flood**—Enables ARP forwarding of nonmatching ARP packets. The ACE forwards all ARP packets to all interfaces in the bridge group. This is the default setting. In the absence of a static ARP entry, this option bridges all packets. With this option, the ACE does not increment the Inspect Failed counter of the `show arp statistics` command.

- **no-flood**—Disables ARP forwarding for the interface and drops nonmatching ARP packets. In the absence of a static ARP entry, this option does not bridge any packets. With this option, the ACE does increment the Inspect Failed counter of the `show arp statistics` command.

For example, to enable ARP inspection and to drop all nonmatching ARP packets, enter:

```
host1/Admin(config)# arp inspection enable no-flood
```

To disable ARP inspection, use the `no arp inspection enable` command. For example, enter:

```
host1/Admin(config)# no arp inspection enable
```

### Configuring the ARP Retry Attempts

By default, the number of ARP attempts before the ACE flags any learned and configured hosts as down is 3. To configure the number of ARP retry attempts, use the `arp retries` command in configuration mode. You configure this command per context. The syntax of this command is as follows:

```
arp retries number
```

The `number` argument is the number of ARP retry attempts. Enter a number from 2 to 15. The default is 3.

For example, to configure a retry attempts at 6, enter:

```
host1/Admin(config)# arp retries 6
```

To reset the number of ARP retry attempts to the default of 3, use the `no arp retries` command. For example, enter:

```
host1/Admin(config)# no arp retries
```
Chapter 4      Configuring ARP

Configuring the ARP Retry Interval

By default, the interval when the ACE sends ARP retry attempts to any learned or configured hosts is 10 seconds. To configure this interval, use the `arp rate` command in configuration mode. You configure this command per context. The syntax of this command is as follows:

```
arp rate seconds
```

The `seconds` argument is the number of seconds between ARP retry attempts to hosts. Enter a number from 1 to 60. The default is 10.

For example, to configure the retry attempt interval of 15 seconds, enter:

```
host1/Admin(config)# arp rate 15
```

To reset the retry attempt interval to the default of 10 seconds, use the `no arp rate` command. For example, enter:

```
host1/Admin(config)# no arp rate
```

Configuring the ARP Request Interval

By default, the refresh interval for existing ARP entries of configured host addresses is 300 seconds. To configure this interval, use the `arp interval` command in configuration mode. You configure this command per context. The syntax of this command is as follows:

```
arp interval seconds
```

The `seconds` argument is the number of seconds between each ARP request sent to the host. Enter a number from 15 to 31536000. The default is 300.

**Note**

When you change the ARP request internal for learned hosts and configured hosts, the new timeout does not take effect until the existing time is reached. If you want the new timeout to take effect immediately, enter the `clear arp` command to apply the new ARP interval (see the “Clearing ARP Learned Entries from the ARP Table” section).
For example, to configure a request period of 15 seconds, enter:

```bash
host1/Admin(config)# arp interval 15
```

To reset the ARP request interval to the default of 300 seconds, use the `no arp interval` command. For example, enter:

```bash
host1/Admin(config)# no arp interval
```

### Enabling the Learning of MAC Addresses

By default, for bridged traffic, the ACE learns MAC addresses from all traffic. For routed traffic, the ACE learns MAC addresses only from ARP response packets or from packets that are destined to the ACE (for example, a ping to a VIP or a ping to a VLAN interface). To enable the ACE to learn MAC addresses from traffic after the command has been disabled, use the `arp learned-mode enable` command in configuration mode. You configure this command per context. This command is enabled by default.

The syntax of this command is as follows:

```bash
arp learned-mode enable
```

For example, to enable the ACE to learn MAC addresses from traffic after the command has been disabled, enter:

```bash
host1/Admin(config)# arp learned-mode enable
```

To instruct the ACE to forward packets without learning the ARP information, use the `no arp learned-mode enable` command. For example, enter:

```bash
host1/Admin(config)# no arp learned-mode enable
```

### Enabling Source MAC Validation

Source MAC validation allows you to instruct the ACE to check the source MAC address in an Ethernet header against the sender’s MAC address in an ARP payload for every ARP packet received by the ACE on the specified interface. The ACE does not learn or update the ARP or MAC tables for packets with different MAC addresses. By default, source MAC validation is disabled.
4-7
Cisco Application Control Engine Module Routing and Bridging Configuration Guide

Chapter 4      Configuring ARP

Configuring the ARP Learned Interval

If ARP inspection fails, then the ACE does not perform source MAC validation. For details about ARP inspection, see the “Enabling ARP Inspection” section.

To configure source MAC validation, use the `arp inspection` command in interface configuration mode. The syntax of this command is:

```
arp inspection validate src-mac [flood | no-flood]
```

The options are as follows:

- `flood`—Enables ARP forwarding for the interface and forwards ARP packets with nonmatching source MAC addresses to all interfaces in the bridge group. This is the default option when you enable source MAC validation.

- `no-flood`—Disables ARP forwarding for the interface and drops ARP packets with nonmatching source MAC addresses.

Regardless of whether you enter the `flood` or the `no-flood` option, if the source MAC address of the ARP packet does not match the MAC address of the Ethernet header, then the source MAC validation fails and the ACE increments the Smac-validation Failed counter of the `show arp statistics` command.

For example, to enable source MAC validation and instruct the ACE to drop ARP packets with nonmatching source MAC addresses, enter the following command:

```
host1/Admin(config-if)# arp inspection validate src-mac no-flood
```

To disable source MAC validation, enter the following command:

```
host1/Admin(config-if)# no arp inspection validate src-mac no-flood
```

Configuring the ARP Learned Interval

By default, the refresh interval for existing ARP entries for learned host addresses is 14400 seconds. To configure this interval, use the `arp learned-interval` command in configuration mode. You configure this command per context. The syntax of this command is as follows:

```
arp learned-interval seconds
```

OL-20816-01
Disabling the Replication of ARP Entries

By default, ARP entry replication is enabled. To disable the replication of ARP entries, use the `arp sync disable` command in configuration mode.

The syntax of this command is as follows:

```
arp sync disable
```

For example, to disable the replication of ARP entries, enter:

```
host1/Admin(config)# arp sync disable
```

To reenable ARP entry replication, use the `no arp sync disable` command. For example, enter:

```
host1/Admin(config)# no arp sync disable
```

Specifying a Time Interval Between ARP Sync Messages

By default, the time interval between ARP synchronization messages for learned hosts is 5 seconds. To specify this time interval, use the `arp sync-interval` command in configuration mode.

The syntax of this command is as follows:

```
arp sync-interval number
```
Configuring the Rate Limit for Gratuitous ARP Packets

By default, the rate limit for gratuitous ARPs sent by the ACE is 512 packets per second. To configure this rate limit, use the `arp ratelimit` command in configuration mode. This command is available only in the Admin context. This rate limit applies to the module and not per context.

The syntax of this command is as follows:

```
arp ratelimit number
```

The `number` argument defines the rate limit as packets per second. Enter an integer from 100 to 8192. The default is 512.

For example, to specify a rate limit of 1000 packets per second, enter:

```
host1/Admin(config)# arp ratelimit 1000
```

To restore the default value of 512 packets per second, use the `no arp ratelimit` command. For example, enter:

```
host1/Admin(config)# no arp ratelimit
```
Displaying ARP Information

You can display ARP address mapping, statistics, and timeout intervals. For more information, see the following topics:

- Displaying IP Address-to-MAC Address Mapping
- Displaying ARP Statistics
- Displaying ARP Inspection Configuration
- Displaying ARP Timeout Values

Note

The `show arp 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*.

Displaying IP Address-to-MAC Address Mapping

To display the current active IP address-to-MAC address mapping in the ARP table, use the `show arp` command in Exec mode. The syntax of this command is as follows:

```
show arp
```

Table 4-1 describes the fields in the `show arp` command output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Context</td>
<td>Current context.</td>
</tr>
<tr>
<td>IP ADDRESS</td>
<td>IP address of the system for ARP mapping.</td>
</tr>
<tr>
<td>MAC-ADDRESS</td>
<td>MAC address of the system mapped to the IP address.</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface name for this entry.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of ARP entry. The possible types are LEARNED,</td>
</tr>
<tr>
<td></td>
<td>GATEWAY, INTERFACE, VSERVER, RSERVER, and NAT.</td>
</tr>
</tbody>
</table>

Table 4-1 Field Descriptions for the show arp Command
Displaying ARP Information

For example, enter:

```
host1/admin# show arp
```

### Displaying ARP Statistics

To display the ARP statistics globally or for a specified VLAN, use the `show arp statistics` command in Exec mode. The syntax of this command is as follows:

```
show arp statistics [vlan vlan_number]
```

The optional `vlan_number` argument displays the ARP statistics for the specified VLAN. Without this option, this command displays the ARP statistics for all VLAN interfaces.

Table 4-2 describes the fields in the `show arp statistics` command output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RX Packets</td>
<td>ARP packets received.</td>
</tr>
<tr>
<td>RX Errors</td>
<td>Number of errors on received ARP packets.</td>
</tr>
<tr>
<td>TX Packets</td>
<td>ARP packets transmitted.</td>
</tr>
<tr>
<td>TX Errors</td>
<td>Number of errors on transmitted ARP packets.</td>
</tr>
<tr>
<td>Bridged Packets</td>
<td>Number of bridged ARP packets.</td>
</tr>
<tr>
<td>Bridged Errors</td>
<td>Number of bridged errors.</td>
</tr>
<tr>
<td>Requests Recvd</td>
<td>ARP requests received.</td>
</tr>
</tbody>
</table>

### Table 4-1 Field Descriptions for the `show arp Command (continued)`

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encap</td>
<td>Pointer to the adjacency entry, if any, for this host; Layer 2 and switch header rewrite information.</td>
</tr>
<tr>
<td>Next ARP(s)</td>
<td>Time in seconds that this dynamic ARP entry is valid.</td>
</tr>
<tr>
<td>Status</td>
<td>State of the system. The possible values are up or down.</td>
</tr>
</tbody>
</table>

For example, enter:

```
host1/admin# show arp
```
Table 4-2  Field Descriptions for the show arp statistics Command Output (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requests Sent</td>
<td>Number of ARP requests sent.</td>
</tr>
<tr>
<td>Response Recvd</td>
<td>ARP responses received.</td>
</tr>
<tr>
<td>Response Sent</td>
<td>Number of ARP responses sent.</td>
</tr>
<tr>
<td>Packets Dropped</td>
<td>Number of dropped ARP packets.</td>
</tr>
<tr>
<td>Inspect Failed</td>
<td>Number of packets failing ARP inspection.</td>
</tr>
<tr>
<td>Collision Detected</td>
<td>Number of detected collisions.</td>
</tr>
<tr>
<td>Gratuitous ARP sent</td>
<td>Number of gratuitous ARP packets sent.</td>
</tr>
<tr>
<td>Hosts learned</td>
<td>Number of hosts learned.</td>
</tr>
<tr>
<td>Smac-validation failed</td>
<td>Number of times that the ACE detected a mismatch between the source MAC address in an Ethernet header and the sender’s MAC address in an ARP payload of a received ARP packet.</td>
</tr>
<tr>
<td>Resolution requests</td>
<td>Number of resolution requests.</td>
</tr>
<tr>
<td>Encap-miss msg</td>
<td>Number of packets that contain no matching ARP entry; each learned ARP entry should correspond to an Encap. When a packet does not have a matching entry, the ACE considers it an Encap miss.</td>
</tr>
<tr>
<td>Pings attempted for Encap-miss msg</td>
<td>Number of times that the ACE recognizes that a ping attempt needs to occur when an Encap miss for a destination packet IP address not on an existing bridge-group subnet occurs.</td>
</tr>
<tr>
<td>Pings quenched for Encap-miss msg</td>
<td>Number of times that the ACE suppresses an effort to ping for the same destination packet IP address if the Encap miss for that address occurs repeatedly and too fast.</td>
</tr>
<tr>
<td>Pings rejected for Encap-miss msg</td>
<td>Number of times that the ACE rejects ping attempts for destination IP addresses when the Encap misses for that address are too many to handle. Similar to the quenched pings, these misses are unique.</td>
</tr>
</tbody>
</table>
Table 4-2 Field Descriptions for the show arp statistics Command Output (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pings Encap-miss responded to</td>
<td>Number of actual pings sent for a missed IP address. The number of this counter should match the number of pings that were attempted for the Encap-miss msg counter.</td>
</tr>
<tr>
<td>Replication Counters</td>
<td></td>
</tr>
<tr>
<td>Msg Received</td>
<td>Number of ARP replication messages that were received by the standby ACE.</td>
</tr>
<tr>
<td>Hosts Replicated</td>
<td>Number of hosts for which ARP replication succeeded and entries were created on the standby.</td>
</tr>
<tr>
<td>Replication Failed</td>
<td>Number of hosts for which replication failed on the standby ACE.</td>
</tr>
<tr>
<td>Replication Ignored</td>
<td>Number of hosts for which replication messages were ignored on the standby, possibly because the entries are already present.</td>
</tr>
</tbody>
</table>

For example, enter:

```
host1/admin# show arp statistics
```

You can also display ARP traffic statistics by using the `show ip traffic` command. This command displays the number of received and sent packets, and associated errors, requests, and responses.

### Displaying ARP Inspection Configuration

To display the ARP inspection configuration, use the `show arp inspection` command in Exec mode. The syntax of this command is as follows:

```
show arp inspection
```
Table 4-3 describes the fields in the `show arp inspection` command output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Context</td>
<td>Name of the current context.</td>
</tr>
<tr>
<td>ARP Inspection</td>
<td>Status of whether ARP inspection is enabled.</td>
</tr>
<tr>
<td>Flooding</td>
<td>Status of whether flooding is enabled.</td>
</tr>
</tbody>
</table>

**Displaying ARP Timeout Values**

To display the ARP timeout values, use the `show arp timeout` command in Exec mode. The syntax of this command is as follows:

```
show arp timeout
```

Table 4-4 describes the fields in the `show arp timeout` command output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refresh Time</td>
<td>Interval in seconds between ARP requests sent to the ACE to validate the cache entry.</td>
</tr>
<tr>
<td>Learned Address</td>
<td>Interval in seconds when the ACE sends ARP requests for learned hosts.</td>
</tr>
<tr>
<td>Configured Address</td>
<td>Interval in seconds that the ACE sends ARP refresh requests for configured hosts. By default, the interval is 300 seconds.</td>
</tr>
<tr>
<td>Retry Rate</td>
<td>Interval in seconds when the ACE sends ARP retry attempts to hosts.</td>
</tr>
<tr>
<td>Max Retries per Host</td>
<td>Number of ARP attempts before the ACE flags the host as down.</td>
</tr>
</tbody>
</table>
Clearing ARP Learned Entries from the ARP Table

To clear the ARP learned entries from the ARP cache table, use the `clear arp` command. The syntax of this command is as follows:

```
clear arp [no-refresh]
```

The optional `no-refresh` keyword clears the learned ARP entries in the cache table without performing an ARP on the entries. Without this option, this command performs an ARP on the entries.

For example, to clear the ARP learned entries with a re-ARP on the entries, enter:

```
host1/Admin# clear arp
```

Clearing ARP Statistics

To clear the ARP statistics counters, use the `clear arp statistics` command. The syntax of this command is as follows:

```
clear arp statistics [vlan number]
```

The optional `vlan number` argument clears the statistic counters for the specified interface. Without this option, this command clears all counters for all interfaces.

For example, to clear the ARP statistics counters globally, enter:

```
host1/Admin# clear arp statistics
```
CHAPTER 5

Configuring the DHCP Relay

This chapter describes how Dynamic Host Configuration Protocol (DHCP) servers provide configuration parameters to DHCP clients. DHCP supplies network settings, including the host IP address, the default gateway, and a DNS server. When DHCP clients and associated servers do not reside on the same IP network or subnet, a DHCP relay agent can transfer DHCP messages between them. The DHCP relay agent operates as the interface between DHCP clients and the server. It listens for client requests and adds vital configuration data, such as the client’s link information, which is needed by the server to allocate the address for the client. When the DHCP server responds, the DHCP relay agent forwards the reply back to the DHCP client.

Note

The ACE does not support DHCP relay for DHCP packets received on shared VLANs between contexts.

This chapter contains the following major sections:

- DHCP Server and Client Overview
- DHCP Relay Configuration Quick Start
- Configuring the DHCP Relay Agent
- Viewing DHCP Relay Configuration and Statistics
DHCP Server and Client Overview

DHCP provides a framework for passing configuration information dynamically to hosts on a TCP/IP network. A DHCP client is an Internet host using DHCP to obtain configuration parameters such as an IP address.

A DHCP relay agent is any host that forwards DHCP packets between clients and servers. Relay agents are used to forward requests and replies between clients and servers when they are not on the same physical subnet. Relay agent forwarding is distinct from the normal forwarding of an IP router, where IP datagrams are switched between networks somewhat transparently. By contrast, relay agents receive DHCP messages and then generate a new DHCP message to send on another interface.

Figure 5-1 shows the basic steps that occur when a DHCP client requests an IP address from a DHCP server. The client, Host A, sends a DHCPDISCOVER broadcast message to locate a DHCP server. A relay agent forwards the packets between the DHCP client and server. A DHCP server offers configuration parameters (such as an IP address, a MAC address, a domain name, and a lease for the IP address) to the client in a DHCPOFFER unicast message.

Figure 5-1   DHCP Request for an IP Address from a DHCP Server
Table 5-1 provides a quick overview of the steps required to configure the DHCP relay function on the ACE. Each step includes the CLI command required to complete the task. For a complete description of each feature and all the options associated with the CLI command, see the sections following Table 5-1.

**Table 5-1 DHCP Relay Configuration Quick Start**

<table>
<thead>
<tr>
<th>Task and Command Example</th>
</tr>
</thead>
</table>
| 1. If you are operating in multiple contexts, observe the CLI prompt to verify that you are operating in the desired context. If necessary, log directly in to, or change to, the correct context.  
host1/Admin# changeto C1  
host1/C1# |
| The rest of the examples in this table use the Admin context unless otherwise specified. For details on creating contexts, see the Cisco Application Control Engine Module Virtualization Configuration Guide. |
| 2. Enter configuration mode by entering config.  
host1/Admin# config  
Enter configuration commands, one per line. End with CNTL/Z  
host1/Admin(config)# |
| 3. Enable the DHCP relay agent to accept DHCP requests from clients on the associated context or VLAN interface.  
host1/Admin(config)# ip dhcp relay enable |
| 4. Specify the IP address of a DHCP server to which the DHCP relay agent forwards client requests.  
host1/Admin(config)# ip dhcp relay server 192.168.20.1 |
| 5. (Optional) Configure a relay agent information reforwarding policy on the DHCP server to identify what the DHCP server should do if a forwarded message already contains relay information.  
host1/Admin(config)# ip dhcp relay information policy replace |
| 6. (Optional) Save your configuration changes to flash memory.  
host1/Admin(config)# exit  
host1/Admin# copy running-config startup-config |
Configuring the DHCP Relay Agent

This section describes how to configure the DHCP relay agent on the ACE. When you configure the ACE as a DHCP relay agent, it is responsible for forwarding the requests and responses that are negotiated between the DHCP clients and the server. By default, the DHCP relay agent is disabled. You must configure a DHCP server when you enable the DHCP relay agent.

You can configure the DHCP relay agent at both the context and VLAN interface levels of the ACE as follows:

- If you configure the DHCP relay agent at the context level, the configuration applies to all interfaces associated with the context.
- If you configure the DHCP relay agent at the VLAN interface level, the configuration applies to that particular interface only; the remaining interfaces revert to the context level configuration.

This section contains the following topics:

- Enabling the DHCP Relay
- Specifying the DHCP Server IP Address
- Configuring a Relay Agent Information Reforwarding Policy

Enabling the DHCP Relay

You can accept DHCP requests from clients on the associated context or VLAN interface and enable the DHCP relay agent by using the `ip dhcp relay enable` command. The DHCP relay starts forwarding packets to the DHCP server address specified in the `ip dhcp relay server` command for the associated VLAN interface or context.

The syntax of this command is as follows:

```
ip dhcp relay enable
```

For example, to enable the DHCP relay to all interfaces associated with a context, enter:

```
host1/Admin(config)# ip dhcp relay enable
```
For example, to enable the DHCP relay at the VLAN interface level, enter:

```
host1/Admin(config)# interface vlan 50
host1/Admin(config-if)# ip dhcp relay enable
```

To disable the DHCP relay for all interfaces associated with a context, enter:

```
host1/Admin(config)# no ip dhcp relay enable
```

To disable the DHCP relay on the VLAN interface, enter:

```
host1/Admin(config-if)# no ip dhcp relay enable
```

### Specifying the DHCP Server IP Address

You can set the IP address of a DHCP server to which the DHCP relay agent forwards client requests by using the `ip dhcp relay server` command.

The syntax of this command is as follows:

```
ip dhcp relay server ip_address
```

The `ip_address` argument specifies the IP address of the DHCP server. Enter the address in dotted-decimal IP notation (for example, 192.168.20.1).

For example, to set the IP address of a DHCP relay server to all interfaces associated with a context, enter:

```
host1/Admin(config)# ip dhcp relay enable
host1/Admin(config)# ip dhcp relay server 192.168.20.1
```

For example, to set the IP address of a DHCP relay server at the VLAN interface level, enter:

```
host1/Admin(config)# interface vlan 50
host1/Admin(config-if)# ip dhcp relay enable
host1/Admin(config-if)# ip dhcp relay server 192.168.20.1
```

To remove the IP address of a DHCP server, enter:

```
host1/Admin(config-if)# no ip dhcp relay server 192.168.20.1
```
Configuring a Relay Agent Information Reforwarding Policy

You can configure the DHCP relay agent to identify the action to perform if a forwarded message already contains relay information by using the `ip dhcp relay information policy` command in configuration mode. By default, the reforwarding policy is to drop the DHCP relay packet.

**Note**

You cannot set the relay agent information reforwarding policy at the VLAN interface level; you can only globally set this function for all interfaces associated with a context.

The syntax of this command is as follows:

```
ip dhcp relay information policy {keep | replace}
```

The keywords are as follows:

- **keep**—Indicates that existing information is left unchanged on the DHCP relay agent.
- **replace**—Indicates that existing information is overwritten on the DHCP relay agent.

For example, to set the relay agent information reforwarding policy to replace existing information for all interfaces associated with a context, enter:

```
host1/Admin(config)# ip dhcp relay information policy replace
```

To restore the default relay information policy to drop the DHCP relay packet, enter:

```
host1/Admin(config)# no ip dhcp relay information policy replace
```
Viewing DHCP Relay Configuration and Statistics

You can view configuration information and statistics collected for the DHCP relay agent by using the `show ip dhcp relay` command. There are three `show` commands for DHCP relay:

- `show ip dhcp relay conf`—Displays the DHCP configuration information.
- `show ip dhcp relay information policy`—Displays the relay agent information reforwarding policy status.
- `show ip dhcp relay statistics`—Displays the DHCP relay statistics.

The output of this command increments until you enter the `clear ip dhcp relay statistics` command.

For example, to display the configured status of the relay agent information reforwarding policy, enter:

```
host/Admin# show ip dhcp relay information policy
DHCP Relay reforwarding policy configured = REPLACE
```

To clear all of the DHCP relay statistics information, use the `clear ip dhcp relay statistics` command. For example, enter:

```
host1/Admin# clear ip dhcp relay statistics
```

Table 5-2 describes the fields in the `show ip dhcp relay conf` command output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Context level config</td>
<td>Configuration information for the DHCP relay agent at the context level.</td>
</tr>
<tr>
<td>Status</td>
<td>Operating status of the DHCP server at the context level: Enabled or Disabled.</td>
</tr>
<tr>
<td>Server</td>
<td>IP address of the DHCP server at the context level.</td>
</tr>
</tbody>
</table>
Table 5-2  
**Field Descriptions for the show ip dhcp relay conf Command Output (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface level configuration</td>
<td>Configuration information for the DHCP relay agent at the VLAN interface level.</td>
</tr>
<tr>
<td>VLAN</td>
<td>Assigned interface VLAN number.</td>
</tr>
<tr>
<td>Interface ID</td>
<td>Interface ID for the VLAN.</td>
</tr>
<tr>
<td>Status</td>
<td>Operating status of the DHCP server at the VLAN interface level: Enabled or Disabled.</td>
</tr>
<tr>
<td>Server</td>
<td>IP address of the DHCP server at the VLAN interface level.</td>
</tr>
</tbody>
</table>

Table 5-3 describes the fields in the `show ip dhcp relay statistics` command output.

Table 5-3  
**Field Descriptions for the show ip dhcp relay statistics Command Output**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Context level configuration</td>
<td>Statistics for the DHCP relay agent at the context level.</td>
</tr>
<tr>
<td>Number of BOOTREQUEST packets relayed</td>
<td>Incremented number of forwarded BOOTREQUEST packets to a DHCP server.</td>
</tr>
<tr>
<td>Number of DHCPDISCOVER packets relayed</td>
<td>Incremented number of forwarded DHCPDISCOVER packets to a DHCP server.</td>
</tr>
<tr>
<td>Number of DHCPREQUEST packets relayed</td>
<td>Incremented number of forwarded DHCPREQUEST packets to a DHCP server.</td>
</tr>
<tr>
<td>Number of DHCPDECLINE packets relayed</td>
<td>Incremented number of forwarded DHCPDECLINE packets to a DHCP server.</td>
</tr>
</tbody>
</table>
### Table 5-3  Field Descriptions for the show ip dhcp relay statistics Command Output (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of DHCPRELEASE packets relayed</td>
<td>Incremented number of forwarded DHCPRELEASE packets to a DHCP server.</td>
</tr>
<tr>
<td>Number of DHCPINFORM packets relayed</td>
<td>Incremented number of forwarded DHCPINFORM packets to a DHCP server.</td>
</tr>
<tr>
<td>Number of BOOTREPLY packets relayed</td>
<td>Incremented number of forwarded BOOTREPLY packets to a DHCP server.</td>
</tr>
<tr>
<td>Number of DHCPOFFER packets relayed</td>
<td>Incremented number of forwarded DHCPOFFER packets to a DHCP server.</td>
</tr>
<tr>
<td>Number of DHCPACK packets relayed</td>
<td>Incremented number of forwarded DHCPACK packets to a DHCP server.</td>
</tr>
<tr>
<td>Number of DHCPNAK packets relayed</td>
<td>Incremented number of forwarded DHCPNAK packets to a DHCP server.</td>
</tr>
<tr>
<td>Number of failures while relaying</td>
<td>Number of failures that occurred while the DHCP relay agent forwarded packets to a DHCP server.</td>
</tr>
<tr>
<td>Interface level configuration</td>
<td>Statistics for the DHCP relay agent at the VLAN interface level.</td>
</tr>
</tbody>
</table>
Addresses, Protocols, and Ports Reference

This appendix provides a quick reference for the following topics:

- IP Addresses and Subnet Masks
- Protocols and Applications
- TCP and UDP Ports
- ICMP Types

IP Addresses and Subnet Masks

This section describes how to use IP addresses in the ACE. An IP address is a 32-bit number written in dotted-decimal notation: four 8-bit fields (octets) converted from binary to decimal numbers, separated by dots. The first part of an IP address identifies the network on which the host resides, while the second part identifies the particular host on the given network. The network number field is called the network prefix. All hosts on a given network share the same network prefix but must have a unique host number. In classful IP, the class of the address determines the boundary between the network prefix and the host number.

This section contains the following topics:

- Classes
- Private Networks
- Subnet Masks
Classes

IP host addresses are divided into three different address classes: Class A, Class B, and Class C. Each class fixes the boundary between the network prefix and the host number at a different point within the 32-bit address. Class D addresses are reserved for multicast IP. The class descriptions are as follows:

- Class A addresses (1.xxx.xxx.xxx through 126.xxx.xxx.xxx) use only the first octet as the network prefix.
- Class B addresses (128.0.xxx.xxx through 191.255.xxx.xxx) use the first two octets as the network prefix.
- Class C addresses (192.0.0.xxx through 223.255.255.xxx) use the first three octets as the network prefix.

Because Class A addresses have 16,777,214 host addresses and Class B addresses have 65,534 hosts, you can use subnet masking to break these huge networks into smaller subnets.

Private Networks

If you need large numbers of addresses on your network, and they do not need to be routed on the Internet, you can use private IP addresses that the Internet Assigned Numbers Authority (IANA) recommends (see RFC 1918). The following address ranges are designated as private networks that should not be advertised:

- 10.0.0.0 through 10.255.255.255
- 172.16.0.0 through 172.31.255.255
- 192.168.0.0 through 192.168.255.255
Subnet Masks

A subnet mask allows you to convert a single Class A, B, or C network into multiple networks. With a subnet mask, you can create an extended network prefix that adds bits from the host number to the network prefix. For example, a Class C network prefix always consists of the first three octets of the IP address. But a Class C extended network prefix uses part of the fourth octet as well.

Subnet masking is easy to understand if you use binary notation instead of dotted-decimal notation. The bits in the subnet mask have a one-to-one correspondence with the Internet address:

- The bits are set to 1 if the corresponding bit in the IP address is part of the extended network prefix.
- The bits are set to 0 if the bit is part of the host number.

Example 1—If you have the Class B address 129.10.0.0 and you want to use the entire third octet as part of the extended network prefix instead of the host number, you must specify a subnet mask of 11111111.11111111.11111111.00000000. This subnet mask converts the Class B address into the equivalent of a Class C address, where the host number consists of the last octet only.

Example 2—If you want to use only part of the third octet for the extended network prefix, then you must specify a subnet mask like 11111111.11111111.11111000.00000000, which uses only 5 bits of the third octet for the extended network prefix.

You can write a subnet mask as a dotted-decimal mask or as a /bits (“slash bits”) mask. In Example 1, for a dotted-decimal mask, you convert each binary octet into a decimal number: 255.255.255.0. For a /bits mask, you add the number of 1s: /24. In Example 2, the decimal number is 255.255.248.0 and the /bits is /21.

You can also combine multiple Class C networks into a larger network—or supernet—by using part of the third octet for the extended network prefix. An example is 192.168.0.0/20.

This section contains the following topics:

- Determining the Subnet Mask
- Determining the Address to Use with the Subnet Mask
Determining the Subnet Mask

To determine the subnet mask based on the number of hosts that you want, see Table A-1.

<table>
<thead>
<tr>
<th>Hosts</th>
<th>/Bits Mask</th>
<th>Dotted-Decimal Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>16,777,216</td>
<td>/8</td>
<td>255.0.0.0 Class A Network</td>
</tr>
<tr>
<td>65,536</td>
<td>/16</td>
<td>255.255.0.0 Class B Network</td>
</tr>
<tr>
<td>32,768</td>
<td>/17</td>
<td>255.255.128.0</td>
</tr>
<tr>
<td>16,384</td>
<td>/18</td>
<td>255.255.192.0</td>
</tr>
<tr>
<td>8,192</td>
<td>/19</td>
<td>255.255.224.0</td>
</tr>
<tr>
<td>4,096</td>
<td>/20</td>
<td>255.255.240.0</td>
</tr>
<tr>
<td>2,048</td>
<td>/21</td>
<td>255.255.248.0</td>
</tr>
<tr>
<td>1,024</td>
<td>/22</td>
<td>255.255.252.0</td>
</tr>
<tr>
<td>512</td>
<td>/23</td>
<td>255.255.254.0</td>
</tr>
<tr>
<td>256</td>
<td>/24</td>
<td>255.255.255.0 Class C Network</td>
</tr>
<tr>
<td>128</td>
<td>/25</td>
<td>255.255.255.128</td>
</tr>
<tr>
<td>64</td>
<td>/26</td>
<td>255.255.255.192</td>
</tr>
<tr>
<td>32</td>
<td>/27</td>
<td>255.255.255.224</td>
</tr>
<tr>
<td>16</td>
<td>/28</td>
<td>255.255.255.240</td>
</tr>
<tr>
<td>8</td>
<td>/29</td>
<td>255.255.255.248</td>
</tr>
<tr>
<td>4</td>
<td>/30</td>
<td>255.255.255.252</td>
</tr>
<tr>
<td>Do not use</td>
<td>/31</td>
<td>255.255.255.254</td>
</tr>
<tr>
<td>1</td>
<td>/32</td>
<td>255.255.255.255 Single Host Address</td>
</tr>
</tbody>
</table>

1. The first and last number of a subnet are reserved, except for /32, which identifies a single host.
Determining the Address to Use with the Subnet Mask

The following sections describe how to determine the network address to use with a subnet mask for a Class C-size and a Class B-size network:

- Class C-Size Network Address
- Class B-Size Network Address

Class C-Size Network Address

For a network between 2 and 254 hosts, the fourth octet falls on a multiple of the number of host addresses, starting with 0. For example, the 8-host subnets (/29) of 192.168.0.x are as follows:

<table>
<thead>
<tr>
<th>Subnet with Mask /29 (255.255.255.248)</th>
<th>Address Range¹</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.0.0</td>
<td>192.168.0.0 to 192.168.0.7</td>
</tr>
<tr>
<td>192.168.0.8</td>
<td>192.168.0.8 to 192.168.0.15</td>
</tr>
<tr>
<td>192.168.0.16</td>
<td>192.168.0.16 to 192.168.0.31</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>192.168.0.248</td>
<td>192.168.0.248 to 192.168.0.255</td>
</tr>
</tbody>
</table>

1. The first and last address of a subnet are reserved. In the first subnet example, you cannot use 192.168.0.0 or 192.168.0.7.

Class B-Size Network Address

To determine the network address to use with the subnet mask for a network that has between 254 and 65,534 hosts, you must determine the value of the third octet for each possible extended network prefix. For example, you might want to subnet an address such as 10.1.x.0, where the first two octets are fixed because they are used in the extended network prefix, and the fourth octet is 0 because all bits are used for the host number.
To determine the value of the third octet, follow these steps:

**Step 1** Calculate how many subnets you can make from the network by dividing 65,536 (the total number of addresses using the third and fourth octet) by the number of host addresses you want.

For example, 65,536 divided by 4096 hosts equals 16 subnets.

Therefore, there are 16 subnets of 4096 addresses each in a Class B-size network.

**Step 2** Determine the multiple of the third octet value by dividing 256 (the number of values for the third octet) by the number of subnets.

In this example, 256/16 = 16.

The third octet falls on a multiple of 16, starting with 0.

Therefore, the 16 subnets of the network 10.1 are as follows:

<table>
<thead>
<tr>
<th>Subnet with Mask /20 (255.255.240.0)</th>
<th>Address Range¹</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.0.0</td>
<td>10.1.0.0 to 10.1.15.255</td>
</tr>
<tr>
<td>10.1.16.0</td>
<td>10.1.16.0 to 10.1.31.255</td>
</tr>
<tr>
<td>10.1.32.0</td>
<td>10.1.32.0 to 10.1.47.255</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>10.1.240.0</td>
<td>10.1.240.0 to 10.1.255.255</td>
</tr>
</tbody>
</table>

¹. The first and last address of a subnet are reserved. In the first subnet example, you cannot use 10.1.0.0 or 10.1.15.255.
Protocols and Applications

This section describes the protocols and applications to help you configure the ACE. The ACE does not pass multicast or routing protocols in routed mode.

Possible literal values are **ah**, **eigrp**, **esp**, **gre**, **icmp**, **igmp**, **igrp**, **ip**, **ipinip**, **nos**, **pcp**, **snp**, **tcp**, and **udp**. You can also specify any protocol by number.

Table A-2 lists the numeric values for the protocol literals.

<table>
<thead>
<tr>
<th>Literal</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ah</td>
<td>51</td>
<td>Authentication Header for IPv6, RFC 1826</td>
</tr>
<tr>
<td>eigrp</td>
<td>88</td>
<td>Enhanced Interior Gateway Routing Protocol</td>
</tr>
<tr>
<td>esp</td>
<td>50</td>
<td>Encapsulated Security Payload for IPv6, RFC 1827</td>
</tr>
<tr>
<td>gre</td>
<td>47</td>
<td>Generic routing encapsulation</td>
</tr>
<tr>
<td>icmp</td>
<td>1</td>
<td>Internet Control Message Protocol, RFC 792</td>
</tr>
<tr>
<td>igmp</td>
<td>2</td>
<td>Internet Group Management Protocol, RFC 1112</td>
</tr>
<tr>
<td>igrp</td>
<td>9</td>
<td>Interior Gateway Routing Protocol</td>
</tr>
<tr>
<td>ip</td>
<td>0</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>ipinip</td>
<td>4</td>
<td>IP-in-IP encapsulation</td>
</tr>
<tr>
<td>nos</td>
<td>94</td>
<td>Network Operating System (Novell’s NetWare)</td>
</tr>
<tr>
<td>pcp</td>
<td>108</td>
<td>Payload Compression Protocol</td>
</tr>
<tr>
<td>snp</td>
<td>109</td>
<td>Sitara Networks Protocol</td>
</tr>
<tr>
<td>tcp</td>
<td>6</td>
<td>Transmission Control Protocol, RFC 793</td>
</tr>
<tr>
<td>udp</td>
<td>17</td>
<td>User Datagram Protocol, RFC 768</td>
</tr>
</tbody>
</table>

Protocol numbers can be viewed online at the IANA website:

http://www.iana.org/assignments/protocol-numbers
TCP and UDP Ports

Table A-3 lists the literal values and port numbers; either can be entered in ACE commands. See the following caveats:

- The ACE uses port 1521 for SQL*Net. This is the default port used by Oracle for SQL*Net. This value, however, does not agree with IANA port assignments.
- The ACE listens for Remote Authentication Dial-In User Service (RADIUS) on ports 1645 and 1646. If your RADIUS server uses the standard ports 1812 and 1813, you can configure the ACE to listen to those ports using the `aaa-server`, `radius-authport`, and `aaa-server radius-acctport` commands.
- To assign a port for Domain Name System (DNS) access, use `domain`, not `dns`. The `dns` keyword translates into the port value for `dnsix`.

Port numbers can be viewed online at the IANA website:
http://www.iana.org/assignments/port-numbers

<table>
<thead>
<tr>
<th>Literal</th>
<th>Protocol</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aol</td>
<td>TCP</td>
<td>5190</td>
<td>America Online</td>
</tr>
<tr>
<td>bgp</td>
<td>TCP</td>
<td>179</td>
<td>Border Gateway Protocol, RFC 1163</td>
</tr>
<tr>
<td>biff</td>
<td>UDP</td>
<td>512</td>
<td>Used by mail system to notify users that new mail is received</td>
</tr>
<tr>
<td>bootpc</td>
<td>UDP</td>
<td>68</td>
<td>Bootstrap Protocol Client</td>
</tr>
<tr>
<td>bootps</td>
<td>UDP</td>
<td>67</td>
<td>Bootstrap Protocol Server</td>
</tr>
<tr>
<td>chargen</td>
<td>TCP</td>
<td>19</td>
<td>Character Generator</td>
</tr>
<tr>
<td>citrix-ica</td>
<td>TCP</td>
<td>1494</td>
<td>Citrix Independent Computing Architecture (ICA) protocol</td>
</tr>
<tr>
<td>cmd</td>
<td>TCP</td>
<td>514</td>
<td>Similar to <code>exec</code> except that <code>cmd</code> has automatic authentication</td>
</tr>
<tr>
<td>ctiqbe</td>
<td>TCP</td>
<td>2748</td>
<td>Computer Telephony Interface Quick Buffer Encoding</td>
</tr>
<tr>
<td>Literal</td>
<td>Protocol</td>
<td>Value</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>----------</td>
<td>-------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>daytime</td>
<td>TCP</td>
<td>13</td>
<td>Day time, RFC 867</td>
</tr>
<tr>
<td>discard</td>
<td>TCP, UDP</td>
<td>9</td>
<td>Discard</td>
</tr>
<tr>
<td>domain</td>
<td>TCP, UDP</td>
<td>53</td>
<td>DNS (Domain Name System)</td>
</tr>
<tr>
<td>dnsix</td>
<td>UDP</td>
<td>195</td>
<td>DNSIX Session Management Module Audit Redirector</td>
</tr>
<tr>
<td>echo</td>
<td>TCP, UDP</td>
<td>7</td>
<td>Echo</td>
</tr>
<tr>
<td>exec</td>
<td>TCP</td>
<td>512</td>
<td>Remote process execution</td>
</tr>
<tr>
<td>finger</td>
<td>TCP</td>
<td>79</td>
<td>Finger</td>
</tr>
<tr>
<td>ftp</td>
<td>TCP</td>
<td>21</td>
<td>File Transfer Protocol (control port)</td>
</tr>
<tr>
<td>ftp-data</td>
<td>TCP</td>
<td>20</td>
<td>File Transfer Protocol (data port)</td>
</tr>
<tr>
<td>gopher</td>
<td>TCP</td>
<td>70</td>
<td>Gopher</td>
</tr>
<tr>
<td>https</td>
<td>TCP</td>
<td>443</td>
<td>Hypertext Transfer Protocol (SSL)</td>
</tr>
<tr>
<td>hostname</td>
<td>TCP</td>
<td>101</td>
<td>NIC Host Name Server</td>
</tr>
<tr>
<td>ident</td>
<td>TCP</td>
<td>113</td>
<td>Ident authentication service</td>
</tr>
<tr>
<td>imap4</td>
<td>TCP</td>
<td>143</td>
<td>Internet Message Access Protocol, version 4</td>
</tr>
<tr>
<td>irc</td>
<td>TCP</td>
<td>194</td>
<td>Internet Relay Chat protocol</td>
</tr>
<tr>
<td>isakmp</td>
<td>UDP</td>
<td>500</td>
<td>Internet Security Association and Key Management Protocol</td>
</tr>
<tr>
<td>kerberos</td>
<td>TCP, UDP</td>
<td>750</td>
<td>Kerberos</td>
</tr>
<tr>
<td>klogin</td>
<td>TCP</td>
<td>543</td>
<td>KLOGIN</td>
</tr>
<tr>
<td>kshell</td>
<td>TCP</td>
<td>544</td>
<td>Korn Shell</td>
</tr>
<tr>
<td>ldap</td>
<td>TCP</td>
<td>389</td>
<td>Lightweight Directory Access Protocol</td>
</tr>
<tr>
<td>ldaps</td>
<td>TCP</td>
<td>636</td>
<td>Lightweight Directory Access Protocol (SSL)</td>
</tr>
<tr>
<td>Literal</td>
<td>Protocol</td>
<td>Value</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>----------</td>
<td>-------</td>
<td>------------------------------------------------------------------</td>
</tr>
<tr>
<td>lpd</td>
<td>TCP</td>
<td>515</td>
<td>Line Printer Daemon—printer spooler</td>
</tr>
<tr>
<td>login</td>
<td>TCP</td>
<td>513</td>
<td>Remote login</td>
</tr>
<tr>
<td>lotusnotes</td>
<td>TCP</td>
<td>1352</td>
<td>IBM Lotus Notes</td>
</tr>
<tr>
<td>mobile-ip</td>
<td>UDP</td>
<td>434</td>
<td>MobileIP-Agent</td>
</tr>
<tr>
<td>nameserver</td>
<td>UDP</td>
<td>42</td>
<td>Host Name Server</td>
</tr>
<tr>
<td>netbios-ns</td>
<td>UDP</td>
<td>137</td>
<td>NetBIOS Name Service</td>
</tr>
<tr>
<td>netbios-dgm</td>
<td>UDP</td>
<td>138</td>
<td>NetBIOS Datagram Service</td>
</tr>
<tr>
<td>netbios-ssn</td>
<td>TCP</td>
<td>139</td>
<td>NetBIOS Session Service</td>
</tr>
<tr>
<td>nntp</td>
<td>TCP</td>
<td>119</td>
<td>Network News Transfer Protocol</td>
</tr>
<tr>
<td>ntp</td>
<td>UDP</td>
<td>123</td>
<td>Network Time Protocol</td>
</tr>
<tr>
<td>pcanywhere-status</td>
<td>UDP</td>
<td>5632</td>
<td>pcAnywhere status</td>
</tr>
<tr>
<td>pcanywhere-data</td>
<td>TCP</td>
<td>5631</td>
<td>pcAnywhere data</td>
</tr>
<tr>
<td>pim-auto-rp</td>
<td>TCP, UDP</td>
<td>496</td>
<td>Protocol Independent Multicast, reverse path flooding, dense mode</td>
</tr>
<tr>
<td>pop2</td>
<td>TCP</td>
<td>109</td>
<td>Post Office Protocol—Version 2</td>
</tr>
<tr>
<td>pop3</td>
<td>TCP</td>
<td>110</td>
<td>Post Office Protocol—Version 3</td>
</tr>
<tr>
<td>ppp</td>
<td>TCP</td>
<td>1723</td>
<td>Point-to-Point Tunneling Protocol</td>
</tr>
<tr>
<td>radius</td>
<td>UDP</td>
<td>1645</td>
<td>Remote Authentication Dial-In User Service</td>
</tr>
<tr>
<td>radius-acct</td>
<td>UDP</td>
<td>1646</td>
<td>Remote Authentication Dial-In User Service (accounting)</td>
</tr>
<tr>
<td>rip</td>
<td>UDP</td>
<td>520</td>
<td>Routing Information Protocol</td>
</tr>
<tr>
<td>secureid-udp</td>
<td>UDP</td>
<td>5510</td>
<td>SecureID over UDP</td>
</tr>
</tbody>
</table>
### Table A-3 Port Literal Values (continued)

<table>
<thead>
<tr>
<th>Literal</th>
<th>Protocol</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>smtp</td>
<td>TCP</td>
<td>25</td>
<td>Simple Mail Transport Protocol</td>
</tr>
<tr>
<td>snmp</td>
<td>UDP</td>
<td>161</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>snmptrap</td>
<td>UDP</td>
<td>162</td>
<td>Simple Network Management Protocol—Trap</td>
</tr>
<tr>
<td>sqlnet</td>
<td>TCP</td>
<td>1521</td>
<td>Structured Query Language Network</td>
</tr>
<tr>
<td>ssh</td>
<td>TCP</td>
<td>22</td>
<td>Secure Shell</td>
</tr>
<tr>
<td>sunrpc (rpc)</td>
<td>TCP, UDP</td>
<td>111</td>
<td>Sun Remote Procedure Call</td>
</tr>
<tr>
<td>syslog</td>
<td>UDP</td>
<td>514</td>
<td>System Log</td>
</tr>
<tr>
<td>tacacs</td>
<td>TCP, UDP</td>
<td>49</td>
<td>Terminal Access Controller Access Control System Plus</td>
</tr>
<tr>
<td>talk</td>
<td>TCP, UDP</td>
<td>517</td>
<td>Talk</td>
</tr>
<tr>
<td>telnet</td>
<td>TCP</td>
<td>23</td>
<td>RFC 854 Telnet</td>
</tr>
<tr>
<td>tftp</td>
<td>UDP</td>
<td>69</td>
<td>Trivial File Transfer Protocol</td>
</tr>
<tr>
<td>time</td>
<td>UDP</td>
<td>37</td>
<td>Time</td>
</tr>
<tr>
<td>uucp</td>
<td>TCP</td>
<td>540</td>
<td>UNIX-to-UNIX Copy Program</td>
</tr>
<tr>
<td>who</td>
<td>UDP</td>
<td>513</td>
<td>Who</td>
</tr>
<tr>
<td>whois</td>
<td>TCP</td>
<td>43</td>
<td>Who Is</td>
</tr>
<tr>
<td>www</td>
<td>TCP</td>
<td>80</td>
<td>World Wide Web</td>
</tr>
<tr>
<td>xdmcp</td>
<td>UDP</td>
<td>177</td>
<td>X Display Manager Control Protocol</td>
</tr>
</tbody>
</table>
ICMP Types

Table A-4 lists the ICMP type numbers and names that you can enter in ACE commands.

<table>
<thead>
<tr>
<th>ICMP Number</th>
<th>ICMP Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>echo-reply</td>
</tr>
<tr>
<td>3</td>
<td>unreachable</td>
</tr>
<tr>
<td>4</td>
<td>source-quench</td>
</tr>
<tr>
<td>5</td>
<td>redirect</td>
</tr>
<tr>
<td>6</td>
<td>alternate-address</td>
</tr>
<tr>
<td>8</td>
<td>echo</td>
</tr>
<tr>
<td>9</td>
<td>router-advertisement</td>
</tr>
<tr>
<td>10</td>
<td>router-solicitation</td>
</tr>
<tr>
<td>11</td>
<td>time-exceeded</td>
</tr>
<tr>
<td>12</td>
<td>parameter-problem</td>
</tr>
<tr>
<td>13</td>
<td>timestamp-request</td>
</tr>
<tr>
<td>14</td>
<td>timestamp-reply</td>
</tr>
<tr>
<td>15</td>
<td>information-request</td>
</tr>
<tr>
<td>16</td>
<td>information-reply</td>
</tr>
<tr>
<td>17</td>
<td>mask-request</td>
</tr>
<tr>
<td>18</td>
<td>mask-reply</td>
</tr>
<tr>
<td>31</td>
<td>conversion-error</td>
</tr>
<tr>
<td>32</td>
<td>mobile-redirect</td>
</tr>
</tbody>
</table>
INDEX

A

ACLs
  bridge-group VLAN, assigning to 3-6
  VLAN interface, assigning to 1-22
addresses
  bank of MAC, configuring for shared VLANs 1-7
  egress MAC lookup, disabling 1-8
IP, range for subnets A-6
MAC, autogenerating 1-17
MAC, learning for ARP 4-6
source MAC validation 4-6
alias IP address
  assigning to a BVI 3-11
  assigning to a VLAN 1-16
alternate address, ICMP message A-12
ARP
  configuring 4-1
  entry replication, disabling 4-8
  inspection, displaying ARP configuration 4-14
  inspection, enabling 4-3
  inspection, enabling ARP 4-3
  inspection configuration, displaying 4-14
IP address-to-MAC address mapping, displaying 4-10
learned entries, clearing 4-16
learned interval, configuring 4-7
MAC address learning 4-6
rate limiting gratuitous ARP packets 4-9
request interval, configuring 4-5
retry attempts, configuring 4-4
retry interval, configuring 4-5
static entry, adding 4-2
statistics, clearing 4-16
statistics, displaying 4-11
time interval between sync messages, specifying 4-8
timeout values, displaying 4-15
autostate, enabling supervisor VLAN notification 1-5

B

bits subnet masks A-4
bridge-group virtual interface 3-2
  ACL, assigning 3-6
  alias IP address, assigning 3-11
  bridge group, assigning 3-5
configuring 3-8
creating 3-8
description 3-13
displaying information on 3-14
enabling 3-13
interface, enabling 3-7
IP address, assigning 3-9
peer IP address, assigning 3-12

bridging 3-1
bridge group, displaying information 3-14
bridge-group virtual interface, configuring 3-8
bridge group VLAN, configuring 3-5
configuration example 3-15
quick start 3-3

c
Class A, B, and C addresses A-2
classes of IP addresses A-2
configuration
  bridging example 3-15
connectivity, verifying 2-5
context
  VLAN, assigning 1-5
conversion error, ICMP message A-12

d
default route 2-3, 2-4
  configuring 2-3
  removing 2-4
DHCP relay
  agent, configuring 5-4
  agent, enabling 5-4
  configuration, displaying 5-7
  configuring 5-1
  information reforwarding policy, configuring 5-6
  overview 5-2
  quick start 5-3
  server IP address, configuring 5-5
  statistics, displaying 5-7
disabling entry replication for ARP 4-8
dotted decimal subnet masks A-4

e
echo, ICMP message A-12
echo reply, ICMP message A-12
egress MAC address lookup, disabling 1-8
enabling traffic flow
  on bridge-group VLAN interface 3-7
  on BVI 3-13
  on VLAN interface 1-13
<table>
<thead>
<tr>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>eobc</strong>, displaying information on</td>
</tr>
<tr>
<td>example</td>
</tr>
<tr>
<td>bridging configuration</td>
</tr>
<tr>
<td><strong>F</strong></td>
</tr>
<tr>
<td>FIB (forward information base), displaying</td>
</tr>
<tr>
<td>forward information base (FIB), displaying</td>
</tr>
<tr>
<td><strong>G</strong></td>
</tr>
<tr>
<td>groups</td>
</tr>
<tr>
<td>VLAN, assigning</td>
</tr>
<tr>
<td>VLAN, creating</td>
</tr>
<tr>
<td><strong>H</strong></td>
</tr>
<tr>
<td>hosts, subnet masks for</td>
</tr>
<tr>
<td><strong>I</strong></td>
</tr>
<tr>
<td>ICMP</td>
</tr>
<tr>
<td>type numbers</td>
</tr>
<tr>
<td>information reforwarding policy, for DHCP</td>
</tr>
<tr>
<td>information reply, ICMP message</td>
</tr>
<tr>
<td>information request, ICMP message</td>
</tr>
<tr>
<td>IP address alias (BVI)</td>
</tr>
<tr>
<td>assigning to BVI</td>
</tr>
<tr>
<td>assigning to VLAN interface</td>
</tr>
<tr>
<td>BVI</td>
</tr>
<tr>
<td>classes</td>
</tr>
<tr>
<td>peer (BVI)</td>
</tr>
<tr>
<td>peer IP, assigning to VLAN interface</td>
</tr>
<tr>
<td>private</td>
</tr>
<tr>
<td>secondary</td>
</tr>
<tr>
<td>subnet mask</td>
</tr>
<tr>
<td>IP address-to-MAC address mapping, displaying</td>
</tr>
<tr>
<td>IP routes, displaying</td>
</tr>
<tr>
<td><strong>L</strong></td>
</tr>
<tr>
<td>learned entries, clearing ARP table</td>
</tr>
<tr>
<td>learned interval, for ARP</td>
</tr>
<tr>
<td><strong>M</strong></td>
</tr>
<tr>
<td>MAC addresses</td>
</tr>
<tr>
<td>assigning a bank for shared VLANs</td>
</tr>
<tr>
<td>autogenerating</td>
</tr>
<tr>
<td>disabling egress lookup</td>
</tr>
<tr>
<td>learning for ARP</td>
</tr>
<tr>
<td>source validation, enabling</td>
</tr>
<tr>
<td>mac-sticky feature, enabling on VLAN interface</td>
</tr>
<tr>
<td>mask reply, ICMP message</td>
</tr>
<tr>
<td>Index</td>
</tr>
<tr>
<td>-------</td>
</tr>
</tbody>
</table>

- mask request, ICMP message  **A-12**
- mobile redirect, ICMP message  **A-12**
- MSFC, adding switched virtual interface to  **1-4**
- **MTU**
  - setting for VLAN interface  **1-14**

**P**

- parameter problem, ICMP message  **A-12**
- peer IP address
  - assigning to an interface  **1-15**
  - assigning to BVI  **3-12**
- policy map
  - assigning to VLAN interface  **1-21**
- private networks, IP addresses  **A-2**
- private VLAN information, displaying  **1-28**
- protocol numbers and literal values  **A-7**

**Q**

- quick start
  - bridge mode configuration  **3-3**
  - DHCP relay  **5-3**

**R**

- rate limiting
  - gratuitous ARP packets  **4-9**
- redirect, ICMP message  **A-12**
- request interval, for ARP  **4-5**
- retry
  - attempts, for ARP  **4-4**
  - interval, for ARP  **4-5**
- RHI, advertising for  **2-4**
- router advertisement, ICMP message  **A-12**
- router solicitation, ICMP message  **A-12**
- routing
  - advertising for RHI  **2-4**
  - default route, configuring  **2-3**
  - default route, removing  **2-4**
  - IP addresses, assigning to interfaces  **2-2**
  - IP routes, displaying  **2-8**
  - verifying connectivity  **2-5**

**S**

- secondary IP address  **1-10**
  - alias  **1-17, 3-11**
  - BVI  **3-10**
  - peer  **1-15, 3-12**
  - VLAN interface  **1-12**
- service policy
  - assigning a policy map  **1-21**
- shared VLAN
  - allocating  **1-6**
  - IP address  **1-11**
  - MAC addresses, assigning a bank of  **1-7**
- source MAC validation, enabling  **4-6**
source quench, ICMP message A-12
specifying an ARP sync message time interval 4-8
static ARP entry 4-2
static route
  configuring 2-3
  removing 2-4
statistics
  ARP, clearing 4-16
  ARP, displaying 4-11
  DHCP relay 5-7
  VLAN, clearing 1-29
subnet masks
  /bits A-4
  address range A-6
  class B size A-5
  class C size A-5
dotted decimal A-4
  number of hosts A-4
  overview A-3
supervisor
  assigning VLAN groups to the ACE 1-3
  displaying VLANS downloaded from 1-28
switched virtual interface, adding to MSFC 1-4

T
TCP
  ports and literal values A-7
time exceeded, ICMP message A-12
timeout values, displaying ARP 4-15
timestamp-reply, ICMP message A-12
timestamp-request, ICMP message A-12
trace routes
  from the ACE 2-6
  on ACE-configured IP addresses 2-7

U
UDP
  ports and literal values A-7
unreachable, ICMP message A-12

V
virtual routed interface, creating for bridge group 3-8
VLANs
  access list, applying 1-22
  alias IP address, setting 1-16
  configuring 1-2
  configuring on ACE 1-9
  configuring on the supervisor 1-2
  context, assigning 1-5
description, defining 1-19
downloaded from supervisor, displaying 1-28
enabling autostate supervisor notification 1-5
eobc information, displaying 1-26
groups, assigning 1-3
groups, creating 1-2
interface manager tables, displaying 1-27
IP addresses, assigning 1-10
mack-sticky, enabling 1-18
MTU, setting 1-14
peer IP addresses, setting 1-15
policy map, assigning 1-21
private information, displaying 1-28
secondary IP addresses 1-11
statistics, clearing 1-29
statistics, displaying 1-23
summary statistics, displaying 1-25
switched virtual interfaces, adding to MSFC 1-4
traffic flow, enabling and disabling 1-13