Interface Configuration Mode Commands

Interface configuration mode commands allow you to configure a VLAN interface or a bridge-group virtual interface (BVI), and, for the ACE appliance, an Ethernet port or a port-channel interface. To configure a bridge-group virtual interface (BVI), Ethernet port, port-channel interface, or VLAN interface, use the interface command. The CLI prompt changes to (config-if). Use the no form of this command to remove the interface from the context. For information about the commands in interface configuration mode, see the following commands.

```
interface {bvi group_number | gigabitEthernet slot_number/port_number | port-channel channel_number | vlan number}

no interface {bvi group_number | gigabitEthernet slot_number/port_number | port-channel channel_number | vlan number}
```

### Syntax Description

**bvi group_number**

- Creates a BVI for a bridge group and accesses interface configuration mode commands for the BVI. The `group_number` argument is the bridge-group number configured on a VLAN interface.

**gigabitEthernet slot_number/port_number**

- (ACE appliance only) Specifies one of the four Ethernet ports on the rear panel of the ACE.
  - `slot_number`—The physical slot on the ACE containing the Ethernet ports. This selection is always 1, the location of the daughter card in the ACE. The daughter card includes the four Layer 2 Ethernet ports to perform Layer 2 switching.
  - `port_number`—The physical Ethernet port on the ACE. Valid selections are 1 through 4, which specifies one of the four Ethernet ports (1, 2, 3, or 4) associated with the slot 1 (daughter card) selection.

**port-channel channel_number**

- (ACE appliance only) Specifies the channel number assigned to this port-channel interface. Valid values are from 1 to 255.

**vlan number**

- Assigns the VLAN to the context and accesses interface configuration mode commands for the VLAN. The `number` argument is the VLAN number you want to assign to the interface. VLAN numbers are 2 to 4094 (VLAN 1 is reserved for internal use and cannot be used).
  - (ACE module only) The VLAN is assigned to the ACE from the supervisor engine for the Catalyst 6500 series switch.

### Command Modes

**Configuration mode**

BVI and VLAN interface—Admin and user contexts

(ACE appliance only) Ethernet port and port-channel interface—Admin context only

### Command History

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0(0)A1(2)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
Usage Guidelines

All commands in this mode require the interface feature in your user role. For details about role-based access control (RBAC) and user roles, see the Virtualization Guide, Cisco ACE Application Control Engine.

To enable the bridge-group VLANs, you must configure a bridge-group virtual interface (BVI) that represents a corresponding bridge group. An IP address in the same subnet should be configured on the BVI. This address is used for management traffic and as a source IP address for traffic from the ACE, similar to ARP requests.

The ACE supports a maximum of 4093 VLAN interfaces with a maximum of 1,024 shared VLANs.

The ACE supports a maximum of 4094 BVI interfaces.

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

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.

You can configure one or more VLAN interfaces in any user context before you assign those VLAN interfaces to the associated user contexts through the (config-context) allocate-interface command in the Admin context.

ACE Appliance Guidelines

In addition, the Ethernet port and port-channel interface command functions require the Admin user role.

The four Ethernet ports provide physical Ethernet ports to connect servers, PCs, routers, and other devices to the ACE. You can configure the four Ethernet ports to provide an interface for connecting to 10-Mbps, 100-Mbps, or 1000-Mbps networks. Each Layer 2 Ethernet port supports autonegotiate, or full-duplex or half-duplex operation on an Ethernet LAN, and can carry traffic within a designated VLAN.

You can group physical ports together on the ACE to form a logical Layer 2 interface called the EtherChannel (or port-channel). All the ports belonging to the same port-channel must be configured with same values; for example, port parameters, VLAN membership, trunk configuration. Only one port-channel in a channel group is allowed, and a physical port can belong to only to a single port-channel interface.

Examples

To assign VLAN interface 200 to the Admin context and access interface configuration mode, enter:

```bash
host1/Admin(config)# interface vlan 200
host1/Admin(config-if)#
```

To remove a VLAN, enter:

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

To create a BVI for bridge group 15, enter:

```bash
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

Related Commands
- show arp
- show interface
- show ip
- show running-config
- show vlans

(config-if) access-group

To apply an IPv6 or an IPv4 access control list (ACL) to the inbound or outbound direction of a VLAN interface and make the ACL active, use the access-group command. Use the no form of this command to remove an ACL from an interface.

```
access-group {input | output} acl_name
no access-group {input | output} acl_name
```

Syntax Description
- **input**: Specifies the inbound direction of the interface to which you want to apply the ACL.
- **output**: Specifies the outbound direction of the interface to which you want to apply the ACL.
- **acl_name**: Identifier of an existing ACL that you want to apply to an interface.

Command Modes
- Interface configuration mode
- Admin and user contexts

Command History

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0(0)A1(2)</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>A5(1.0)</td>
<td>Added IPv6 support.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(7)</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>A5(1.0)</td>
<td>Added IPv6 support.</td>
</tr>
</tbody>
</table>
Usage Guidelines

You must apply ACLs to a VLAN interface to allow the traffic to pass on an interface. You can apply one IPv6 and one IPv4 ACL of each type (extended and EtherType) to both directions of the interface. For connectionless protocols, you need to apply the ACL to the source and destination interfaces if you want traffic to pass in both directions. For example, you can allow Border Gateway Protocol (BGP) in an ACL in transparent mode, and you need to apply the ACL to both interfaces.

A bridge-group VLAN supports extended ACLs for IP traffic and EtherType ACLs for non-IP traffic. For non-IP traffic, you can 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), IP version 6 (IPv6), and bridge protocol data units (BDPUs).

The output option is not allowed for EtherType ACLs.

To apply an ACL globally to all interfaces in a context, use the (config) access-group command.

Examples

To apply an ACL named INBOUND to the inbound direction of an interface, enter:

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

To remove an ACL from an interface, enter:

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

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show access-list</td>
<td></td>
</tr>
<tr>
<td>(config) access-group</td>
<td></td>
</tr>
<tr>
<td>(config) access-list extended</td>
<td></td>
</tr>
</tbody>
</table>

(config-if) alias

To configure an IP address that is shared between active and standby ACEs for a bridge-group virtual interface (BVI) or VLAN interface, use the alias command. Use the no form of this command to delete an alias IP address.

```
alias {ipv6_address [prefix_length] [eui64 | unique-local]} | {ip_address mask [secondary]}
```

```
no alias {ipv6_address [prefix_length] [eui64 | unique-local]} | {ip_address mask [secondary]}
```

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6_address</td>
<td>IPv6 address of the interface.</td>
</tr>
<tr>
<td>/prefix_length</td>
<td>(Optional, except for EUI-64) Specifies how many of the most significant bits (MSBs) of the IPv6 address are used for the network identifier. Enter a a forward slash character (/) followed by an integer from 1 to 128. The default is /128. If you use the optional eui64 keyword, you must specify a prefix length and the prefix must be less than or equal to 64.</td>
</tr>
<tr>
<td>eui64</td>
<td>(Optional) Specifies that the low order 64 bits are automatically generated in the IEEE 64-bit Extended Unique Identifier (EUI-64) format specified in RFC 2373. To use this keyword, you must specify a prefix length, the prefix must be less than or equal to 64, and the host segment must be all zeros.</td>
</tr>
</tbody>
</table>
### Command Modes

Interface configuration mode

Admin and user contexts

### Command History

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0(0)A1(2)</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>A2(3.0)</td>
<td>The <code>secondary</code> option was added.</td>
</tr>
<tr>
<td>A2(3.1)</td>
<td>The number of secondary addresses increased from 4 to 15.</td>
</tr>
<tr>
<td>A4(1.0)</td>
<td>The number of secondary addresses decreased from 15 to 4.</td>
</tr>
<tr>
<td>A4(1.1)</td>
<td>The number of secondary addresses increased from 4 to 15.</td>
</tr>
<tr>
<td>A5(1.0)</td>
<td>Added IPv6 support.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(7)</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>A4(1.0)</td>
<td>The <code>secondary</code> option was added.</td>
</tr>
<tr>
<td>A4(1.1)</td>
<td>The number of secondary addresses increased from 4 to 15.</td>
</tr>
<tr>
<td>A5(1.0)</td>
<td>Added IPv6 support.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

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

For stealth firewalls, an ACE balances traffic among unique VLAN alias IP address interfaces on another ACE that provides paths through stealth firewalls. You configure a stealth firewall so that all traffic moving in both directions across that VLAN moves through the same firewall.

For details about firewall load balancing (FWLB), see the *Server Load-Balancing Guide, Cisco ACE Application Control Engine*.

You cannot configure secondary IP addresses on FT VLANs.

### Examples

To configure an alias IP address and mask, enter:

```
host1/Admin(config-if)# alias 12.0.0.81 255.0.0.0
```

To configure a secondary alias IP address, enter:

```
host1/Admin(config-if)# alias 193.168.12.15 255.255.255.0 secondary
```
To remove an alias IP address, enter:
host1/Admin(config-if)# no alias 192.168.12.15 255.255.255.0

To remove a secondary alias IP address, enter:
host1/Admin(config-if)# no alias 193.168.12.15 255.255.255.0 secondary

Related Commands show interface

(config-if) arp

To add a static ARP entry in the ARP table for a VLAN interface, use the arp command. Use the no form of this command to remove a static ARP entry.

\[
\text{arp } \text{ip_address mac_address} \\
\text{no arp } \text{ip_address mac_address}
\]

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip_address</td>
<td>IP address for an ARP table entry. Enter the IP address in dotted-decimal notation (for example, 172.16.27.1).</td>
</tr>
<tr>
<td>mac_address</td>
<td>MAC address for the ARP table entry. Enter the MAC address in dotted-hexadecimal notation (for example, 00.02.9a.3b.94.d9).</td>
</tr>
</tbody>
</table>

Command Modes Interface configuration mode

Admin and user contexts

Command History

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0(0)A1(2)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(7)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines Static ARPs for bridged interfaces are configured on the specific interface.

Examples

To allow ARP responses from the router at 10.1.1.1 with the MAC address 00.02.9a.3b.94.d9, enter:

\[
\text{host1/Admin(config-if)# arp 10.1.1.1 00.02.9a.3b.94.d9}
\]

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

\[
\text{host1/Admin(config-if)# no arp 10.1.1.1 00.02.9a.3b.94.d9}
\]
Related Commands

**show arp**

### (config-if) arp inspection

To enable the ACE to dynamically 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, use the **arp inspection** command. Use the **no** form of this command to remove a static ARP entry.

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

```
norarp ip_address mac_address
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>validate src-mac</th>
<th>Instructs 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</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>flood</strong></td>
<td>(Optional) 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 dynamic ARP inspection.</td>
<td></td>
</tr>
<tr>
<td><strong>no-flood</strong></td>
<td>(Optional) Disables ARP forwarding for the interface and drops ARP packets with nonmatching source MAC addresses.</td>
<td></td>
</tr>
</tbody>
</table>

**Command Modes**

- Interface configuration mode
- Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0(0)A1(6.3)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(7)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The ACE does not learn or update the ARP or MAC tables for packets with different MAC addresses. By default, dynamic ARP inspection is disabled. If you enable this feature, the default option is **flood**. Use this feature for interoperability with third-party firewalls (for example, CheckPoint).

If ARP inspection fails, then the ACE does not perform source MAC validation. For details about ARP inspection, see the **(config) arp** command.

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** command.
**Examples**

To enable 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 and to forward (flood) the packets, enter:

```
host1/Admin(config-if)# arp inspection validate src-mac
```

To restore the behavior of the ACE to the default of not validating source MAC addresses, enter the following command:

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

**Related Commands**

`show arp`
(config-if) bridge-group

To assign the VLAN to a bridge group, use the bridge-group command. Use the no form of this command to remove the bridge group from the VLAN.

```
bridge-group number

no bridge-group
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>Bridge-group number. Enter an integer from 1 to 4094.</td>
</tr>
</tbody>
</table>

**Command Modes**

Interface configuration mode

Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0(0)A1(2)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(7)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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, VLANs do not have configured IP addresses.

To enable the bridge-group VLANs, you must configure a bridge-group virtual interface (BVI) that represents a corresponding bridge group.

**Examples**

To assign bridge group 15 to the VLAN, enter:

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

To remove the bridge group from the VLAN, enter:

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

**Related Commands**

- show interface
(config-if) carrier-delay

(ACE appliance only) To add a configurable delay at the physical port level to address issues with transition time, based on the variety of peers, use the `carrier-delay` command. Use the `no` form of the command to remove the carrier delay for the Ethernet port.

```
carrier-delay seconds
no carrier-delay seconds
```

**Syntax Description**

| seconds | The carrier transition delay in seconds. Valid values are 0 to 120 seconds. The default is 0 (no carrier delay).

**Command Modes**

| Interface configuration mode
| Admin context only

**Command History**

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(8)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If you connect an ACE to a Catalyst 6500 series switch, your configuration on the Catalyst may include the Spanning Tree Protocol (STP). However, the ACE does not support STP. In this case, you may find that the Layer 2 convergence time is much longer than the physical port up time. For example, the physical port would normally be up within 3 seconds, but STP moving to the forward state may need approximately 30 seconds. During this transitional time, although the ACE declares the port to be up, the traffic will not pass.

The `carrier-delay` command adds a configurable delay at the physical port level to address this transition time, based on the variety of peers.

**Examples**

To add a configurable delay of 60 seconds at the physical port level for Ethernet port 3, enter:

```
host1/Admin(config)# interface gigabitEthernet 1/3
host1/Admin(config-if)# carrier-delay 60
```

To remove the carrier delay for the Ethernet port, enter:

```
host1/Admin(config-if)# no carrier-delay 60
```

**Related Commands**

`show interface`
(config-if) channel-group

(ACE appliance only) To map the physical Ethernet port to a port channel when configuring Layer 2 EtherChannels, use the channel-group command. Use the no form of the command to remove the channel group assigned to the Ethernet port.

```
channel-group channel_number
no channel-group channel_number
```

**Syntax Description**

| channel_number | Channel number assigned to this channel group. Valid values are from 1 to 255. |

**Command Modes**

Interface configuration mode

Admin context only

**Command History**

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(7)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You can group physical ports together on the ACE to form a logical Layer 2 interface called the EtherChannel (or port-channel). The channel-group command configures the Ethernet port in a port-channel group and automatically creates the port-channel logical interface.

It is not necessary to configure a port-channel interface before assigning a physical Ethernet port to a channel group through the channel-group command. A port-channel interface is created automatically when the channel group receives its first physical interface, if it is not already created.

**Examples**

To create a channel group with a channel number of 255, enter:

```
host1/Admin(config)# interface gigabitEthernet 1/3
host1/Admin(config)# channel-group 255
```

To remove the channel group assigned to the Ethernet port, enter:

```
host1/Admin(config-if)# no channel-group 255
```

**Related Commands**

show interface
(config-if) description

To provide a description for a bridge-group virtual interface (BVI) or VLAN interface, use the `description` command. Use the `no` form of this command to delete the description.

```
description text

no description
```

**Syntax Description**

- `text`: Description for the interface. Enter an unquoted text string that contains a maximum of 240 characters including spaces.

**Command Modes**

- Interface configuration mode
- Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0(0)A1(2)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(7)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command has no usage guidelines.

**Examples**

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, enter:

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

**Related Commands**

- `show interface`
(config-if) duplex

(ACE appliance only) To configure an Ethernet port for full- or half-duplex operation, use the `duplex` command in interface configuration mode. The default configuration for an ACE interface is autonegotiate. Use the `no` form of this command to revert to autonegotiation operation.

```
duplex {full | half}
```

```
no duplex
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>full</td>
<td>Configures the specified Ethernet port for full-duplex operation, which allows data to travel in both directions at the same time.</td>
</tr>
<tr>
<td>half</td>
<td>Configures the specified Ethernet port for half-duplex operation. A half-duplex setting ensures that data travels only in one direction at any given time.</td>
</tr>
</tbody>
</table>

**Command Modes**

Interface configuration mode
Admin context only

**Command History**

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(7)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If you configure the Ethernet port speed to `auto` on a 10/100/1000-Mbps Ethernet port, both speed and duplex are autonegotiated. The ACE prevents you from making a duplex setting when you configure the speed of an Ethernet port to `auto`. The `speed` command must be a non-auto setting of 10, 100, or 1000 Mbps to be able to configure the duplex setting for the Ethernet port.

**Examples**

To set the duplex mode to full on Ethernet port 3, enter:

```
host1/Admin(config)# interface gigabitEthernet 1/3
host1/Admin(config-if)# duplex full
```

To restore the default setting of autonegotiate for an Ethernet port, enter:

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

**Related Commands**

`(config-if) speed`
(config-if) fragment chain

To configure the maximum number of fragments that belong to the same packet that the ACE accepts for reassembly for a VLAN interface, use the fragment chain command. Use the no form of this command to reset the default value.

```
fragment chain number

no fragment chain
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>number</code></td>
<td>Maximum number of fragments that belong to the same packet. Enter an integer from 1 to 256. The default is 24.</td>
</tr>
</tbody>
</table>

**Command Modes**

Interface configuration mode

Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0(0)A1(2)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(7)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command has no usage guidelines.

**Examples**

To configure a fragment chain limit of 126, enter:

```
host1/C1(config-if)# fragment chain 126
```

To reset the maximum number of fragments in a packet to the default of 24, enter:

```
host1/C1(config-if)# no fragment chain
```

**Related Commands**

show fragment

(config-if) fragment min-mtu

(config-if) fragment timeout
(config-if) fragment min-mtu

To configure the minimum fragment size that the ACE accepts for reassembly for a VLAN interface, use the `fragment min-mtu` command. Use the `no` form of this command to reset the default value.

```
fragment min-mtu number
no fragment min-mtu
```

**Syntax Description**
- `number`: Minimum fragment size. Enter an integer from 28 to 9216 bytes. The default is 576 bytes.

**Command Modes**
- Interface configuration mode
- Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0(0)A1(2)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(7)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
- This command has no usage guidelines.

**Examples**

To configure a minimum fragment size of 1024, enter:

```
host1/C1(config-if)# fragment min-mtu 1024
```

To reset the minimum fragment size to the default value of 576 bytes, enter:

```
host1/C1(config-if)# no fragment min-mtu
```

**Related Commands**
- `show fragment`
- `(config-if) fragment chain`
- `(config-if) fragment timeout`
(config-if) fragment timeout

To configure a reassembly timeout for a VLAN interface, use the fragment timeout command. Use the no form of this command to reset the default value.

```
fragment timeout seconds
```

```
no fragment timeout
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>Reassembly timeout in seconds. Enter an integer from 1 to 30. The default is 5.</td>
</tr>
</tbody>
</table>

**Command Modes**

- Interface configuration mode
- Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0(0)A1(2)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(7)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The IP reassembly timeout specifies the period of time after which the ACE abandons the fragment reassembly process if it does not receive any outstanding fragments for the current fragment chain (fragments that belong to the same packet).

**Examples**

To configure an IP reassembly timeout of 15 seconds, enter:

```
host1/C1(config-if)# fragment timeout 15
```

To reset the fragment timeout to the default value of 5 seconds, enter:

```
host1/C1(config-if)# no fragment timeout
```

**Related Commands**

- `show fragment`
- `(config-if) fragment chain`
- `(config-if) fragment min-mtu`
(config-if) ft-port vlan

(ACE appliance only) To configure one of the Ethernet ports or a port-channel interface on the ACE for fault tolerance using a dedicated FT VLAN for communication between the members of an FT group, use the `ft-port vlan` command in interface configuration mode. Use the `no` form of this command to remove the FT VLAN function from an Ethernet port or port-channel interface.

```
ft-port vlan number

no ft-port vlan number
```

- **Syntax Description**
  - `number`: Unique identifier for the FT VLAN. Valid values are from 2 to 4094.

- **Command Modes**
  - Interface configuration mode
  - Admin context only

- **Command History**
<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(7)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

- **Usage Guidelines**
  Peer ACE appliances communicate with each other over a dedicated FT VLAN. These redundant peers use the FT VLAN to transmit and receive heartbeat packets and state and configuration replication packets.

  On both peer ACE appliances, you must configure the same Ethernet port or the same port-channel interface as the FT VLAN port. For example, if you configure ACE appliance 1 to use Ethernet port 4 as the FT VLAN port, then be sure to configure ACE appliance 2 to use Ethernet port 4 as the FT VLAN port.

  It is not necessary to create an FT VLAN before designating an Ethernet port or port-channel interface as the FT VLAN port.

  When you specify the `ft-port vlan` command, the ACE modifies the associated Ethernet port or port-channel interface to a trunk port.

  We recommend that you enable QoS on the FT VLAN port to provide higher priority for FT traffic (see the `(config-if) qos trust cos` command).

  For details on configuring redundant ACE appliances, including an FT VLAN, see the `Administration Guide, Cisco ACE Application Control Engine`.

- **Examples**
  To configure FT VLAN identifier 60 for Ethernet port 3, enter:

  ```
  host1/Admin(config)# interface gigabitEthernet 1/3
  host1/Admin(config-if)# ft-port vlan 60
  ```

  To remove the FT VLAN from the Ethernet port, enter:

  ```
  host1/Admin(config-if)# no ft-port vlan 60
  ```

- **Related Commands**
  - `show interface`
**icmp-guard**

To enable the ICMP security checks in the ACE after they have been disabled, use the `icmp-guard` command. This feature is enabled by default. Use the `no` form of this command to disable the ICMP security checks.

```
icmp-guard
no icmp-guard
```

### Syntax Description

This command has no keywords or arguments.

### Command Modes

- Interface configuration mode
- Admin and user contexts

### Command History

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0(0)A1(2)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(7)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

By default, the ACE provides several ICMP security checks by matching ICMP reply packets with request packets and using mismatched packets to detect attacks. Also, the ACE forwards ICMP error packets only if a connection record pertaining to the flow for which the error packet was received exists.

**Caution**

If you disable the ACE ICMP security checks, you may expose your ACE and your data center to potential security risks. After you enter the `no icmp-guard` command, the ACE no longer performs Network Address Translation (NAT) translations on the ICMP header and payload in error packets, which potentially can reveal real host IP addresses to attackers.

If you want to operate your ACE as a load balancer only, use the `no icmp-guard` command to disable the ACE ICMP security checks. You must also disable TCP normalization by using the `no normalization` command. For details about operating your ACE for load balancing only, see the *Server Load-Balancing Guide, Cisco ACE Application Control Engine*.

### Examples

To enable the ACE ICMP security checks after you have disabled them, enter:

```
host1/Admin(config)# interface vlan 200
host1/Admin(config-if)# icmp-guard
```

To disable ACE ICMP security checks, enter:

```
host1/Admin(config-if)# no icmp-guard
```
Related Commands

(config-if) normalization
(config-if) ip address

To assign an IPv6 or an IPv4 address to a bridge-group virtual interface (BVI) or a VLAN interface, use the `ip address` command. Use the `no` form of this command to remove an IP address from an interface.

```
ip address {ipv6_address [prefix_length] [eui64 | link-local | unique-local]} | {ipv4_address mask [secondary]}

no ip address {ipv6_address [prefix_length] [eui64 | link-local | unique-local]} | {ipv4_address mask [secondary]}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6_address</td>
<td>IPv6 address of the interface.</td>
</tr>
<tr>
<td>/prefix_length</td>
<td>(Optional, except for EUI-64) Specifies how many of the most significant bits (MSBs) of the IPv6 address are used for the network identifier. Enter a forward slash character (/) followed by an integer from 1 to 128. The default is /128. If you use the optional eui64 keyword, you must specify a prefix length and the prefix must be less than or equal to 64.</td>
</tr>
<tr>
<td>eui64</td>
<td>(Optional) Specifies that the low order 64 bits are automatically generated in the IEEE 64-bit Extended Unique Identifier (EUI-64) format specified in RFC 2373. To use this keyword, you must specify a prefix length, the prefix must be less than or equal to 64, and the host segment must be all zeros.</td>
</tr>
<tr>
<td>link-local</td>
<td>(Optional) Specifies that the address is valid only for the current link.</td>
</tr>
<tr>
<td>unique-local</td>
<td>(Optional) Specifies that this address is globally unique and used only for local communications within a site or organization.</td>
</tr>
<tr>
<td>ipv4_address</td>
<td>IPv4 address of the interface.</td>
</tr>
<tr>
<td>mask</td>
<td>Subnet mask of the interface.</td>
</tr>
<tr>
<td>secondary</td>
<td>(Optional) Configures the address as a secondary IPv4 address allowing multiple subnets under the same interface. You can configure a maximum of 15 secondary addresses per interface. The ACE has a system limit of 1,024 secondary addresses.</td>
</tr>
</tbody>
</table>

**Command Modes**

Interface configuration mode

Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0(0)A1(2)</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>A2(3.0)</td>
<td>The <code>secondary</code> option was added.</td>
</tr>
<tr>
<td>A2(3.1)</td>
<td>The number of secondary addresses increased from 4 to 15.</td>
</tr>
<tr>
<td>A4(1.0)</td>
<td>The number of secondary addresses decreased from 15 to 4.</td>
</tr>
<tr>
<td>A4(1.1)</td>
<td>The number of secondary addresses increased from 4 to 15.</td>
</tr>
<tr>
<td>A5(1.0)</td>
<td>Added IPv6 support.</td>
</tr>
</tbody>
</table>
Usage Guidelines

To process IPv6 traffic on an interface, you must configure the `ipv6 enable` command on that interface. You can configure one IPv6 link-local and one IPv6 local-unique address on an interface. If you configure additional addresses of either type, the existing address is overwritten.

**Caution**

Do not configure under a real server a peer IPv6 address that is calculated from EUI64. In a redundant configuration, if you configure a peer IPv6 address as EUI64 on an interface, the address will not be learned by the active member of an FT group because the address is calculated only on the peer. If you then configure the same calculated IPv6 address on the active under a real server, the CLI accepts it because it does not calculate it. This IPv6 address is not synced to the standby because it conflicts with the interface address. If you subsequently apply a probe to the real server, the state of the real server is PROBE-FAILED on the active and OUTOFSERVICE on the standby. This same check applies to VIPs, routes, interfaces, and probes.

When you assign an IPv4 address to an interface, the ACE automatically makes the interface routed. You must configure a primary IPv4 address for the interface to allow a VLAN to become active. The primary address must be active before a secondary address can be active.

An interface can have only one primary IPv4 address.

When you configure access to an interface, the ACE applies it to all IPv4 addresses configured on the interface.

The ACE treats the secondary addresses the same as a primary address and handles IP broadcasts and ARP requests for the subnet that is assigned to the secondary address as well as the interface routes in the IP routing table.

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

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.

You must configure static ARP entries for bridged interfaces on the specific interface.

In a single context, you must configure each interface address on a unique subnet; the addresses cannot overlap. However, the IP subnet can overlap an interface in different contexts.

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

No routing occurs across contexts even when shared VLANs are configured.

---

### ACE Appliance Release Modification

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(7)</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>A4(1.0)</td>
<td>The <code>secondary</code> option was added.</td>
</tr>
<tr>
<td>A4(1.1)</td>
<td>The number of secondary addresses increased from 4 to 15.</td>
</tr>
<tr>
<td>A5(1.0)</td>
<td>Added IPv6 support.</td>
</tr>
</tbody>
</table>
Examples

IPv6 Examples
To configure an IPv6 link-local address on VLAN 100, enter the following commands:

```
host1/Admin(config)# interface VLAN 100
host1/Admin(config-if)# ip address FE80:DB8:1::1 link-local
```

To remove a link-local address from an interface, enter the following commands:

```
host1/Admin(config)# interface VLAN 100
host1/Admin(config-if)# no ip address FE80:DB8:1::1 link-local
```

IPv4 Examples
To set the IPv4 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
```

To assign a secondary IP address and mask 193.168.1.1 255.255.255.0 to VLAN interface 200, enter the following command:

```
host1/Admin(config-if)# ip address 192.168.1.2 255.255.255.0 secondary
```

To remove the IP address for the VLAN, enter:

```
host1/Admin(config-if)# no ip address 192.168.1.1 255.255.255.0
```

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

```
host1/Admin(config-if)# no ip address 192.168.1.2 255.255.255.0 secondary
```

Related Commands

- `show arp`
- `show interface`
- `show ip`
Interface Configuration Mode Commands

Chapter 2 CLI Commands

Interface Configuration Mode Commands

(config-if) ip df

To configure how the ACE handles an IP packet that has its Don’t Fragment (DF) bit set on a VLAN interface, use the ip df command. Use the no form of this command to instruct the ACE to ignore the DF bit.

```
ip df {clear | allow}
no ip df
```

Syntax Description

<table>
<thead>
<tr>
<th>clear</th>
<th>Clears the DF bit and permits the packet. If the packet is larger than the next-hop maximum transmission unit (MTU), the ACE fragments the packet.</th>
</tr>
</thead>
<tbody>
<tr>
<td>allow</td>
<td>Permits the packet with the DF bit set. This is the default. If the packet is larger than the next-hop MTU, the ACE discards the packet and sends an ICMP unreachable message to the source host.</td>
</tr>
</tbody>
</table>

Command Modes

Interface configuration mode
Admin and user contexts

Command History

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0(0)A1(2)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

ACE Appliance Release

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(7)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Occasionally, an ACE may receive a packet that has its DF bit set in the IP header. This flag tells network routers and the ACE not to fragment the packet and to forward it in its entirety.

Examples

To clear the DF bit and permit the packet, enter:

```
host1/Admin(config-if)# ip df clear
```

To instruct the ACE to ignore the DF bit, enter:

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

Related Commands

This command has no related commands.
(config-if) ip dhcp relay enable

To accept Dynamic Host Configuration Protocol (DHCP) requests on a VLAN interface, use the `ip dhcp relay enable` command. Use the `no` form of this command to disable DHCP on the interface.

```
  ip dhcp relay enable
  no ip dhcp relay enable
```

**Syntax Description**
This command has no keywords or arguments.

**Command Modes**
Interface configuration mode
Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0(0)A1(2)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**ACE Appliance Release**

<table>
<thead>
<tr>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
The DHCP relay starts forwarding packets to the DHCP server address specified in the `ip dhcp relay server` command for the associated interface or context.

**Examples**
To enable the DHCP relay on the interface, enter:

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

To disable the DHCP relay on the interface, enter:

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

**Related Commands**
- (config-if) ip dhcp relay enable
- (config-if) ip dhcp relay server
(config-if) ip dhcp relay server

To set the IP address of a Dynamic Host Configuration Protocol (DHCP) server to which the DHCP relay agent forwards client requests on a VLAN interface, use the `ip dhcp relay server` command. Use the `no` form of this command to remove the IP address of the DHCP server.

```
  ip dhcp relay server ip_address
  no ip dhcp relay server ip_address
```

**Syntax Description**

- `ip_address`: IP address of the DHCP server. Enter the address in dotted-decimal IP notation (for example, 192.168.11.1).

**Command Modes**

- Interface configuration mode
- Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0(0)A1(2)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(7)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command has no usage guidelines.

**Examples**

To specify the IP address for the DHCP relay server, enter:

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

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

```
host1/Admin(config-if)# no ip dhcp relay server 192.168.20.1
```

**Related Commands**

This command has no related commands.
(config-if) ip options

To configure how the ACE handles IP options and to perform specific actions when an IP option is set in a packet for a VLAN interface, use the **ip options** command. Use the **no** form of this command to instruct the ACE to ignore the IP option.

```
ip options {allow | clear | clear-invalid | drop}

no ip options
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>allow</td>
<td>Allows the packet with the IP options set.</td>
</tr>
<tr>
<td>clear</td>
<td>Clears the specified option from the packet and allows the packet.</td>
</tr>
<tr>
<td>clear-invalid</td>
<td>Clears all IP options from the packet if the ACE encounters one or more invalid or unsupported IP options and allows the packet. This option is the default.</td>
</tr>
<tr>
<td>drop</td>
<td>Causes the ACE to discard the packet.</td>
</tr>
</tbody>
</table>

### Command Modes

Interface configuration mode

Admin and user contexts

### Command History

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0(0)A1(2)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(7)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

This command has no usage guidelines.

### Examples

To allow packets with IP options set, enter:

```
host1/Admin(config-if)# ip options allow
```

To reset the ACE to its default of clearing all IP options if the ACE encounters one or more invalid or unsupported IP options, enter:

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

### Related Commands

This command has no related commands.
(config-if) ip route inject vlan

(ACE module only) To advertise a VLAN for route health injection (RHI) that is different from the VIP interface VLAN, use the **ip route inject vlan** command. By default, the ACE advertises the VLAN of the VIP interface for RHI. Use the **no** form of this command to restore the ACE default behavior of advertising the VIP interface VLAN for RHI.

```plaintext
ip route inject vlan vlan_id

no ip route inject vlan vlan_id
```

**Syntax Description**

| **vlan_id** | Interface shared between the supervisor and the intervening device. Enter the ID as an integer from 2 to 4090. |

**Command Modes**

Interface configuration mode

Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A2(1.0)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command when there is no directly shared VLAN between the ACE and the Catalyst 6500 series supervisor. 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.

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

**Examples**

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
```

**Related Commands**

This command has no related commands.
(config-if) ip ttl minimum

To set the packet time-to-live (TTL) hops in the IP header on a VLAN interface, use the `ip ttl minimum` command. By default, the ACE does not rewrite the TTL value of a packet. Use the `no` form of this command to reset the default behavior.

```
ip ttl minimum number
no ip ttl minimum
```

**Syntax Description**
- `number`: Minimum number of hops that a packet can take to reach its destination. Enter an integer from 1 to 255 seconds.

**Command Modes**
- Interface configuration mode
- Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0(0)A1(2)</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>A5(1.0)</td>
<td>Added IPv6 support.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(7)</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>A5(1.0)</td>
<td>Added IPv6 support.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Each router along the packet’s path decrements the TTL by one. If the packet’s TTL equals 0 before the packet reaches its destination, the packet is discarded.

If the TTL value of the incoming packet is lower than the configured minimum value, the ACE rewrites the TTL with the configured value. Otherwise, the ACE transmits the packet with its TTL unchanged or discards the packet if the TTL equals zero. This command applies to both IPv4 and IPv6 flows. The configured value replaces the TTL in an IPv4 packet and the hop limit in an IPv6 packet if the original value is lower.

**Examples**

To set the TTL hops to 15, enter:
```
host1/Admin(config-if)# ip ttl minimum 15
```

To instruct the ACE to ignore the TTL value, enter:
```
host1/Admin(config-if)# no ip ttl minimum
```

**Related Commands**

This command has no related commands.
(config-if) ip verify reverse-path

To enable reverse-path forwarding (RPF) based on the source IP address for a VLAN interface, use the `ip verify reverse-path` command. By default, URPF is disabled on the interface. Use the `no` form of this command to reset the default behavior.

```
ip verify reverse-path
no ip verify reverse-path
```

**Syntax Description**
This command has no keywords or arguments.

**Command Modes**
Interface configuration mode
Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0(0)A1(2)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(7)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Unicast reverse-path forwarding (URPF) helps to mitigate problems caused by the introduction of malformed or forged (spoofed) IP source addresses into a network by allowing the ACE to discard IP packets that lack a verifiable source IP address. This feature enables the ACE to filter both ingress and egress packets to verify addressing and route integrity. The route lookup is typically based on the destination address, not the source address.

When you enable URPF, the ACE discards packets if no route is found or if the route does not match the interface on which the packet arrived.

You cannot use this command when RPF based on the source MAC address for a VLAN interface is enabled through the `(config-if) mac-sticky enable` command.

**Examples**
To enable RPF, enter:

```
host/Admin(config-if)# ip verify reverse-path
```

To disable RPF, enter:

```
host/Admin(config-if)# no ip verify reverse-path
```

**Related Commands**
`(config-if) mac-sticky enable`
(config-if) ipv6 dhcp relay enable

To configure the ACE to accept DHCP requests from IPv6 clients on the associated context or VLAN interface and enable the DHCP relay agent, use the `ipv6 dhcp relay enable` command. Use the `no` form of this command to disable DHCP relay on the specified context or interface.

```
ipv6 dhcp relay enable
no ipv6 dhcp relay enable
```

**Syntax Description**  
This command has no keywords or arguments.

**Command Modes**  
Configuration mode and interface configuration mode  
Admin and user contexts

**Command History**  

<table>
<thead>
<tr>
<th>ACE Module/Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A5(1.0)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**  
This command has no usage guidelines.

**Examples**  
To enable the DHCP relay agent globally for all VLAN interfaces associated with a context, enter the following command:

```
host1/Admin(config)# ipv6 dhcp relay enable
```

To enable the DHCP relay agent at the VLAN interface level, enter the following command:

```
host1/Admin(config)# ipv6 dhcp relay enable
host1/Admin(config)# interface vlan 100
host1/Admin(config-if)# ipv6 dhcp relay enable
```

To disable the DHCP relay agent globally for VLAN interfaces in a context where DHCP relay is not explicitly configured, enter the following command:

```
host1/Admin(config)# no ipv6 dhcp relay enable
```

To disable the DHCP relay agent on a VLAN interface, enter the following commands:

```
host1/Admin(config)# interface vlan 100
host1/Admin(config-if)# no ipv6 dhcp relay enable
```

**Related Commands**  
`show ipv6`  
(config-if) `ipv6 dhcp relay fwd-interface`  
(config-if) `ipv6 dhcp relay server`
(config-if) ipv6 dhcp relay fwd-interface

To configure a forwarding VLAN interface that the ACE uses to forward DHCP requests, use the `ipv6 dhcp relay fwd-interface` command. Use the `no` form of this command to remove the forwarding VLAN interface from the configuration.

```
ipv6 dhcp relay fwd-interface vlan vlan_id

no ipv6 dhcp relay fwd-interface vlan vlan_id
```

**Syntax Description**

```
<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan vlan_id</td>
<td>Specifies the VLAN interface number that the ACE uses to forward DHCP requests. Enter the number of an existing VLAN interface as an integer from 2 to 4094.</td>
</tr>
</tbody>
</table>
```

**Command Modes**

- Configuration mode and interface configuration mode
- Admin and user contexts

**Command History**

```
<table>
<thead>
<tr>
<th>ACE Module/Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A5(1.0)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
```

**Usage Guidelines**

When you configure this command, the ACE uses the specified VLAN interface to forward all client DHCP requests to the All_DHCP_Relay_Agents_and_Servers address of FF02::1:2.

**Examples**

To configure VLAN200 as the DHCP forwarding VLAN interface, enter the following command:

```
host1/Admin(config)# ipv6 dhcp relay fwd-interface vlan 200
```

To remove the forwarding VLAN interface from the configuration, enter the following command:

```
host1/Admin(config)# no ipv6 dhcp relay fwd-interface vlan 200
```

**Related Commands**

- `show ipv6`
- `(config-if) ipv6 dhcp relay enable`
- `(config-if) ipv6 dhcp relay server`
(config-if) ipv6 dhcp relay server

To set the IP address of a DHCP server to which the DHCP relay agent forwards client requests, use the `ipv6 dhcp relay server` command. Use the `no` form of this command to remove the IPv6 address of a DHCP server from a VLAN interface.

```
ipv6 dhcp relay server ipv6_address [fwd-interface vlan vlan_id]
no ipv6 dhcp relay server ipv6_address [fwd-interface vlan vlan_id]
```

### Syntax Description
- `ipv6_address`: Specifies the IPv6 address of the destination DHCPv6 server.
- `fwd-interface vlan vlan_id`: (Optional) Specifies the outgoing forwarding interface if the DHCP server address is a link-local address.

### Command Modes
- Configuration mode and interface configuration mode
- Admin and user contexts

### Command History
ACE Module/Appliance Release  Modification
A5(1.0) This command was introduced.

### Usage Guidelines
This command has no usage guidelines.

### Examples
To set the IPv6 address of a DHCPv6 relay server globally for all interfaces associated with a context, enter:

```
host1/Admin(config)# ipv6 dhcp relay enable
host1/Admin(config)# ipv6 dhcp relay server 2001:DB8:1::1/64
```

To set the IPv6 address of a DHCP relay server at the VLAN interface level, enter:

```
host1/Admin(config)# interface vlan 50
host1/Admin(config-if)# ipv6 dhcp relay enable
host1/Admin(config-if)# ipv6 dhcp relay server 2001:DB8:1::1/64
```

To set the IPv6 address of a DHCPv6 server that is reachable on its link-local address, enter the following commands:

```
host1/Admin(config)# interface vlan 50
host1/Admin(config-if)# ipv6 dhcp relay enable
host1/Admin(config-if)# ipv6 dhcp relay server fe80::250:56ff:fe90:2c fwd-interface vlan 100
```

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

```
host1/Admin(config)# interface vlan 50
host1/Admin(config-if)# no ipv6 dhcp relay server 2001:DB8:1::1/64
```
Related Commands

- `show ipv6`
- `(config-if) ipv6 dhcp relay enable`
- `(config-if) ipv6 dhcp relay fwd-interface`
(config-if) ipv6 enable

To enable IPv6 on an interface, use the **ipv6 enable** command. By default, IPv6 is disabled on an interface. Use the **no** form of this command to reset the default behavior. The syntax of this command is as follows:

```
ipv6 enable
no ipv6 enable
```

**Syntax Description**

This command has no keywords or arguments.

**Command Modes**

Interface configuration mode
Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>ACE Module/Appliance</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A5(1.0)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The interface cannot be in bridged mode. The interface may or may not have IPv4 addresses configured on it.

**Examples**

To enable IPv6 processing on an interface, enter:

```
host/Admin(config-if)# ipv6 enable
```

To disable IPv6 processing on an interface, enter:

```
host/Admin(config-if)# no ipv6 enable
```
(config-if) ipv6 extension-header

To configure how the ACE processes IPv6 extension headers, use the `ipv6 extension-header` command. Use the no form of this command to return the ACE behavior to the default of dropping packets that contain an extension header with an invalid option.

```
ipv6 extension-header {allow | clear | clear-invalid | drop}

no ipv6 extension-header {allow | clear | clear-invalid | drop}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>allow</td>
<td>If a packet contains an IPv6 extension header, the ACE allows the packet with all the header options</td>
</tr>
<tr>
<td>clear</td>
<td>If a packet contains an IPv6 extension header, the ACE clears all the IPv6 extension header options and allows the packet</td>
</tr>
<tr>
<td>clear-invalid</td>
<td>If a packet contains an IPv6 extension header and one of the header options is invalid, the ACE clears all the extension header options and allows the packet</td>
</tr>
<tr>
<td>drop</td>
<td>(Default) If the packet contains an IPv6 extension header and one of the header options is invalid, the ACE drops the packet</td>
</tr>
</tbody>
</table>

**Command Modes**

Interface configuration mode
Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>ACE Module/Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A5(1.0)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The default option is drop. There is no provision to selectively choose which extension header to act on.

**Examples**

To configure the ACE to clear IPv6 extension headers and allow the packet, enter the following commands:

```
host1/Admin(config)# interface vlan 200
host1/Admin(config-if)# ipv6 extension-header clear
```

To reset the behavior of the ACE to the default of dropping packets with invalid IPv6 extension headers, enter the following command:

```
host1/Admin(config-if)# no ipv6 extension-header
```
(config-if) **ipv6 fragment chain**

To configure the maximum number of fragments belonging to the same packet that the ACE accepts for reassembly, use the `ipv6 fragment chain` command. Use the `no` form of this command to reset the maximum number of fragments in a packet to the default of 24.

```
ipv6 fragment chain number

no ipv6 fragment chain number
```

**Syntax Description**

| **number** | Specifies the fragment chain limit as an integer from 1 to 256 fragments. The default is 24 fragments. |

**Command Modes**

Interface configuration mode

Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>ACE Module/Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A5(1.0)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The default option is `drop`. There is no provision to selectively choose which extension header to act on.

**Examples**

To set the IPv6 fragment chain limit as 48, enter the following command:

```
host1/C1(config-if)# ipv6 fragment chain 48
```

To reset the maximum number of fragments in a packet to the default of 24, enter the following command:

```
host1/C1(config-if)# no ipv6 fragment chain
```

**Related Commands**

- (config-if) `ipv6 fragment min-mtu`
- (config-if) `ipv6 fragment timeout`
(config-if) ipv6 fragment min-mtu

To configure the minimum fragment size that the ACE accepts for reassembly, use the `ipv6 fragment min-mtu` command. Use the `no` form of this command to reset the minimum fragment size to the default value of 1280 bytes.

```
ipv6 fragment min-mtu number

no ipv6 fragment min-mtu number
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>number</code></td>
<td>Specifies the minimum fragment size as an integer from 68 to 1280 bytes. The default is 1280 bytes.</td>
</tr>
</tbody>
</table>

**Command Modes**

Interface configuration mode

Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>ACE Module/Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A5(1.0)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command has no usage guidelines.

**Examples**

To configure the minimum IPv6 fragment size that the ACE accepts for reassembly, enter the following command:

```
host1/C1(config-if)# ipv6 fragment min-mtu 1024
```

To reset the minimum fragment size to the default value of 1280 bytes, enter the following command:

```
host1/C1(config-if)# no ipv6 fragment min-mtu
```

**Related Commands**

- (config-if) ipv6 fragment chain
- (config-if) ipv6 fragment timeout
(config-if) ipv6 fragment timeout

To configure the IPv6 reassembly timeout, use the `ipv6 fragment timeout` command. Use the `no` form of this command to reset the fragment timeout to the default value of 60 seconds.

```
ipv6 fragment timeout seconds

no ipv6 fragment timeout seconds
```

Syntax Description

- `seconds`: Specifies the fragment reassembly timeout. Enter an integer from 1 to 60 seconds. The default is 60 seconds.

Command Modes

- Interface configuration mode
- Admin and user contexts

Command History

<table>
<thead>
<tr>
<th>ACE Module/Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A5(1.0)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

The IPv6 reassembly timeout specifies the period of time after which the ACE abandons the fragment reassembly process if it does not receive any outstanding fragments for the current fragment chain (fragments that belong to the same packet).

Examples

To set the fragment reassembly timeout to 30 seconds, enter the following command:

```
host1/C1(config-if)# ipv6 fragment timeout 30
```

To reset the fragment timeout to the default value of 60 seconds, enter the following command:

```
host1/C1(config-if)# no ipv6 fragment timeout
```
(config-if) ipv6 icmp-guard

To enable the ICMP security checks in the ACE after they have been disabled, use the `ipv6 icmp-guard` command. This feature is enabled by default. Use the `no` form of this command to disable the ICMP security checks.

```
ipv6 icmp-guard

no ipv6 icmp-guard
```

**Syntax Description**

This command has no keywords or arguments.

**Command Modes**

- Interface configuration mode
- Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>ACE Module/Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A5(1.0)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `no` form of this command as part of an overall strategy to operate the ACE as a pure server load balancer. For details, see Chapter 1, Overview, in the *Server Load-Balancing Guide, Cisco ACE Application Control Engine*.

The ACE provides several ICMP security checks by matching ICMP reply packets with request packets and using mismatched packets to detect attacks. Also, the ACE forwards ICMP error packets only if a connection record exists pertaining to the flow for which the error packet was received. By default, the ACE ICMP security checks are enabled.

**Caution**

Disabling the ACE ICMPv6 security checks may expose your ACE and your data center to potential security risks. After you enter the `no ipv6 icmp-guard` command, the ACE no longer performs NAT translations on the ICMPv6 header and payload in error packets, which potentially can reveal real host IPv6 addresses to attackers.

When the `ipv6 icmp-guard` command is enabled, only the “Packet Too Big” ICMPv6 message is allowed. To allow other ICMPv6 error messages (for example, the “Time Exceeded” message or the “Parameter Problem” message), the `ipv6 icmp-guard` command should be disabled.

**Examples**

To disable ICMPv6 security checks on interface VLAN 100, enter:
```
host1/C1(config)# interface vlan 100
host1/C1(config-if)# no ipv6 icmp-guard
```

To reenable ICMPv6 security checks, enter:
```
host1/C1(config-if)# ipv6 icmp-guard
```
Related Commands  

(\texttt{config-if}) \texttt{ipv6 normalization}
(config-if) ipv6 mtu

To specify the maximum transmission unit (MTU) for an IPv6 VLAN interface, use the `ipv6 mtu` command. This command allows you to set the data size that is sent on a Layer 3 IPv6 connection. Use the `no` form of this command to reset the MTU block size to the default of 1500 bytes for Layer 3 interfaces.

```
ipv6 mtu bytes

no ipv6 mtu
```

**Syntax Description**
- `bytes` Number of bytes in the MTU. Enter a number from 1280 to 9216 bytes. The default is 1500.

**Command Modes**
- Interface configuration mode
- Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>ACE Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A5(1.0)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The default MTU is a 1500-byte block for Layer 3 interfaces. This value is sufficient for most applications, but you can pick a lower number if network conditions require it. The ACE fragments packets that are larger than the MTU value before sending them to the next hop.

This command is valid only for Layer 3 interfaces (VLANs or BVIs). The ACE will not recognize this command on a transparent (Layer 2) interface.

**Examples**

To specify the MTU data size of for a Layer 3 interface, enter the following command:

```
host1/admin(config-if)# ipv6 mtu 1300
```

To reset the MTU block size to the default value of 1500 for Layer 3 interfaces, enter:

```
host1/admin(config-if)# no ipv6 mtu
```

**Related Commands**
- `show interface`
(config-if) ipv6 nd dad-attempts

To set the number of times that the ACE solicits its neighbors for duplicate address detection (DAD) information on the local link, use the `ipv6 nd dad-attempts` command. Use the `no` form of this command to reset the ACE behavior to the default of sending NS messages for DAD once.

```
ipv6 nd dad-attempts number

no ipv6 nd dad-attempts number
```

### Syntax Description

| `number` | Specifies the number of times that the ACE sends NS messages to its neighbors on the local link for DAD. Enter an integer from 0 to 255. The default is 1. |

### Command Modes

- Interface configuration mode
- Admin and user contexts

### Command History

<table>
<thead>
<tr>
<th>ACE Module/Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A5(1.0)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

This command has no usage guidelines.

### Examples

To configure the ACE to send NS messages three times for DAD, enter the following commands:

```
host1/Admin(config)# interface vlan 100
host1/Admin(config-if)# ipv6 nd dad-attempts 3
```

To reset the ACE behavior to the default of sending NS messages for DAD once, enter the following command:

```
host1/Admin(config-if)# no ipv6 nd dad-attempts
```
(config-if) ipv6 nd managed-config-flag

To instruct the ACE to notify hosts that they should use Dynamic Host Configuration Protocol (DHCP) for address configuration, use the `ipv6 nd managed-config-flag` command. Use the `no` form of this command to reset the ACE behavior to the default of not notifying hosts to use DHCP.

`ipv6 nd managed-config-flag`

`no ipv6 nd managed-config-flag`

**Syntax Description**
This command has no keywords or arguments.

**Command Modes**
Interface configuration mode
Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>ACE Module/Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A5(1.0)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
This command has no usage guidelines.

**Examples**
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
```

**Related Commands**
This command has no related commands.
(config-if) ipv6 nd ns-interval

To configure the interval at which the ACE sends neighbor solicitation (NS) messages for duplicate address detection (DAD) attempts, use the `ipv6 nd ns-interval` command. Use the `no` form of this command to reset the NS interval to the default value of 1000 msecs.

```
ipv6 nd ns-interval interval

no ipv6 nd ns-interval interval
```

**Syntax Description**

- **ns-interval**: Indicates the frequency of the neighbor solicitation (NS) messages that are sent by the ACE.
- **interval**: Specifies the frequency in milliseconds (msecs) of the NS messages that are sent by the ACE. Enter an integer from 1000 to 2147483647. The default is 1000 msecs.

**Command Modes**

- Interface configuration mode
- Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>ACE Module/Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A5(1.0)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The ACE sends neighbor solicitation messages via ICMPv6 on the local link to determine the IPv6 addresses of nearby nodes (hosts or routers).

**Examples**

To configure an NS frequency of 36000 msecs, enter the following commands:

```
host1/Admin(config)# interface VLAN 100
host1/Admin(config-if)# ipv6 nd ns-interval 36000
```

To reset the NS interval to the default value of 1000 msecs, enter the following commands:

```
host1/Admin(config)# interface VLAN 100
host1/Admin(config-if)# no ipv6 nd ns-interval 36000
```

**Related Commands**

- `(config) ipv6 nd interval`
(config-if) ipv6 nd other-config-flag

To notify hosts that they should use DHCP for nonaddress configurations, use the `ipv6 nd other-config-flag` command. Use the `no` form of this command to reset the ACE behavior to the default of not notifying hosts to use DHCP for nonaddress configurations.

```
ipv6 nd other-config-flag
no ipv6 nd other-config-flag
```

**Syntax Description**

This command has no keywords or arguments.

**Command Modes**

- Interface configuration mode
- Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>ACE Module/Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A5(1.0)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command has no usage guidelines.

**Examples**

To instruct hosts to use DHCP for nonaddress configurations, enter the following commands:

```
host1/Admin(config)# interface vlan 100
host1/Admin(config-if)# ipv6 nd other-config-flag
```

To reset the ACE behavior to the default of not notifying hosts to use DHCP for nonaddress configurations, enter the following command:

```
host1/Admin(config-if)# no ipv6 nd other-config-flag
```
(config-if) ipv6 nd prefix

To configure the prefixes that the ACE advertises in RA messages on the local link, use the `ipv6 nd prefix` command. Use the `no` form of this command to remove the prefix from RA messages.

```
ipv6 nd prefix ipv6_address/prefix_length [no-advertise | no-autoconfig | off-link | [pref-lt | valid-lt {number | infinite}]]
```

```
no ipv6 nd prefix ipv6_address/prefix_length [no-advertise | no-autoconfig | off-link | [pref-lt | valid-lt {number | infinite}]]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6_address</code></td>
<td>Specifies the prefix that the ACE advertises in RA messages.</td>
</tr>
<tr>
<td><code>prefix_length</code></td>
<td></td>
</tr>
<tr>
<td><code>no-advertise</code></td>
<td>(Optional) Instructs the ACE to not advertise the prefix.</td>
</tr>
<tr>
<td><code>no-autoconfig</code></td>
<td>(Optional) Specifies that the prefix should not be used for autoconfiguration.</td>
</tr>
<tr>
<td><code>off-link</code></td>
<td>(Optional) Flag related to the L-bit as defined in RFC 2461. When you specify the optional <code>off-link</code> keyword, the L-bit flag is turned off, which indicates that the specified prefix should not be used for on-link determination. However, when the L-bit is enabled (the default setting), it indicates in the router advertisement messages that the specified prefix is assigned to the local link. Therefore, nodes sending traffic to addresses that contain the specified prefix consider the destination to be locally reachable on the link.</td>
</tr>
<tr>
<td><code>valid-lt number</code></td>
<td><code>pref-lt number</code>—(Optional) Length of time in seconds that prefix is preferred. For the <code>number</code> argument, enter an integer from 0 to 2147483647. The default is 604800 (seven days).</td>
</tr>
<tr>
<td><code>valid-lt number</code></td>
<td><code>valid-lt number</code>—(Optional) Length of time in seconds that the prefix is valid. For the <code>number</code> argument, enter an integer from 0 to 2147483647. The default is 2592000 seconds (30 days).</td>
</tr>
<tr>
<td><code>infinite</code></td>
<td>(Optional) Specified that the prefix never expires.</td>
</tr>
</tbody>
</table>

**Command Modes**

Interface configuration mode
Admin and user contexts

**Command History**

ACE Module/Appliance Release | Modification
--- | ---
A5(1.0) | This command was introduced.

**Usage Guidelines**

You can configure a maximum of two prefixes for RA.

**Examples**

To configure the prefixes that the ACE advertises in RA messages, enter the following commands:

```
host1/Admin(config)# interface vlan 100
host1/Admin(config-if)# ipv6 nd prefix 2001:DB8::2/64 valid-lt 3000000
```

To remove the prefix from RA messages, enter the following command:
host1/Admin(config-if)# no ipv6 nd prefix 2001:DB8:1::2/64 valid-lt 3000000

Related Commands
(config-if) ipv6 nd ra hop-limit

To configure the hop limit in the IPv6 header that the ACE’s neighbors should use when originating IPv6 packets, use the `ipv6 nd ra hop-limit` command. Use the `no` form of this command to reset the hop limit to the default value of 64.

```
ipv6 nd ra hop-limit number

no ipv6 nd ra hop-limit number
```

**Syntax Description**
- `number`: Specifies the number of hops that neighbors should use when they originate IPv6 packets. Enter an integer from 0 to 255. The default is 64.

**Command Modes**
- Interface configuration mode
- Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>ACE Module/Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A5(1.0)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
This command has no usage guidelines.

**Examples**
To configure the number of hops that neighbors should use when originating IPv6 packets, enter the following command:

```
host1/Admin(config)# interface vlan 100
host1/Admin(config-if)# ipv6 nd ra hop-limit 32
```

To reset the hop limit to the default of 64, enter the following command:

```
host1/Admin(config-if)# no ipv6 nd ra hop-limit 32
```

**Related Commands**
- `(config-if) ipv6 nd ra interval`
- `(config-if) ipv6 nd ra lifetime`
- `(config-if) ipv6 nd ra suppress`
(config-if) ipv6 nd ra interval

To configure the rate at which the ACE sends router advertisement (RA) messages, use the `ipv6 nd ra interval` command. Use the `no` form of this command to reset the interval to the default of 600 seconds (10 minutes).

```
ipv6 nd ra interval number

no ipv6 nd ra interval number
```

**Syntax Description**

- `number` specifies the rate in seconds at which the ACE sends RA messages to other nodes on the local link. Enter an integer from 4 to 1800. The default is 600.

**Command Modes**

- Interface configuration mode
- Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>ACE Module/Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A5(1.0)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command has no usage guidelines.

**Examples**

To configure the ACE to send RA messages every 900 seconds (15 minutes), enter the following command:

```
host1/Admin(config)# interface vlan 100
host1/Admin(config-if)# ipv6 nd ra interval 900
```

To reset the interval to the default of 600 seconds (10 minutes), enter the following command:

```
host1/Admin(config-if)# no ipv6 nd ra interval
```

**Related Commands**

- `(config-if) ipv6 nd ra hop-limit`
- `(config-if) ipv6 nd ra lifetime`
- `(config-if) ipv6 nd ra suppress`
(config-if) ipv6 nd ra lifetime

The router advertisement (RA) lifetime is the length of time that neighboring nodes should consider the ACE as the default router before they send RS messages again. To configure the RA lifetime, use the `ipv6 nd ra lifetime` command. Use the `no` form of this command to reset the interval to the default of 600 seconds (10 minutes).

```
  ipv6 nd ra lifetime number

  no ipv6 nd ra lifetime number
```

### Syntax Description

- **number**: Specifies the length of time in seconds that the neighboring nodes should consider the ACE as the default router. Enter an integer from 0 to 9000. The default is 1800 seconds (30 minutes).

### Command Modes

- Interface configuration mode
- Admin and user contexts

### Command History

<table>
<thead>
<tr>
<th>ACE Module/Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A5(1.0)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

This command has no usage guidelines.

### Examples

To configure an RA lifetime of 2400 seconds (40 minutes), enter the following commands:

```
  host1/Admin(config)# interface vlan 100
  host1/Admin(config-if)# ipv6 nd ra lifetime 2400
```

To reset the RA lifetime to the default of 1800 seconds (30 minutes), enter the following command:

```
  host1/Admin(config-if)# no ipv6 nd ra lifetime
```

### Related Commands

- `(config-if) ipv6 nd ra hop-limit`
- `(config-if) ipv6 nd ra interval`
- `(config-if) ipv6 nd ra suppress`
To configure the ACE to not respond to router solicitation (RS) messages, use the `ipv6 nd ra suppress` command. Use the `no` form of this command to return the ACE to the default behavior of automatically responding to RS messages.

```
ipv6 nd ra suppress

no ipv6 nd ra suppress
```

### Syntax Description
This command has no keywords or arguments.

### Command Modes
Interface configuration mode

Admin and user contexts

### Command History

<table>
<thead>
<tr>
<th>ACE Module/Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A5(1.0)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines
This command has no usage guidelines.

### Examples
To configure the ACE to not send RA messages to neighbors in response to RS messages, enter the following commands:

```
host1/Admin(config)# interface vlan 100
host1/Admin(config-if)# ipv6 nd ra suppress
```

To reset the ACE behavior to the default of always sending RA messages in response to RS messages, enter the following commands:

```
host1/Admin(config)# interface vlan 100
host1/Admin(config-if)# no ipv6 nd ra suppress
```

### Related Commands
```
(config-if) ipv6 nd ra hop-limit
(config-if) ipv6 nd ra interval
(config-if) ipv6 nd ra lifetime
```
(config-if) ipv6 nd reachable-time

To configure the neighbor reachable time, use the `ipv6 nd reachable-time` command. Use the `no` form of this command to reset the reachable time value to the default of 0 milliseconds (msecs).

```
ipv6 nd reachable-time number
no ipv6 nd reachable-time number
```

**Syntax Description**

| number | Specifies the length of time in milliseconds (msecs) after which a node is considered reachable. Enter an integer from 0 to 3600000 msecs. The default is 0. |

**Command Modes**

- Interface configuration mode
- Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>ACE Module/Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A5(1.0)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The reachable time parameter specifies the time in milliseconds during which a host considers a peer as reachable following the host’s receipt of a reachability confirmation from the peer. A reachability confirmation can be an NA or NS message or any upper protocol traffic. The ACE sends the reachable time value in RA messages in response to RS messages.

**Examples**

To configure the ACE to send a reachable time value of 2000 msecs, enter the following commands:

```
host1/Admin(config)# interface vlan 100
host1/Admin(config-if)# ipv6 nd reachable-time 2000
```

To restore the reachable time value to the default of 1000 msecs, enter the following command:

```
host1/Admin(config-if)# no ipv6 nd reachable-time
```
(config-if) ipv6 nd retransmission-time

To configure the time during which NS messages (including DAD) are retransmitted, use the `ipv6 nd retransmission-time` command. Use the `no` form of this command to restore the NS retransmission time value to the default of 0 milliseconds (msecs).

```
ipv6 nd retransmission-time number
no ipv6 nd retransmission-time number
```

**Syntax Description**

| number | Specifies the time in seconds during which NS messages are retransmitted. Enter an integer from 0 to 3600000. The default is 0. |

**Command Modes**

- Interface configuration mode
- Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>ACE Module/Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A5(1.0)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The ND retransmission time is related to RA and applies to hosts.

**Examples**

To configure the NS retransmission time for hosts, enter the following commands:

```
host1/Admin(config)# interface vlan 100
host1/Admin(config-if)# ipv6 nd retransmission-time 1000
```

To restore the NS retransmission time value to the default of 0 msecs, enter the following command:

```
host1/Admin(config-if)# no ipv6 nd retransmission-time
```
(config-if) ipv6 neighbor

To configure a static ND entry that maps an IPv6 address to a Layer 2 address, use the `ipv6 neighbor` command. Use the `no` form of this command to remove the static ND entry.

```
ipv6 neighbor ipv6_address mac_address
no ipv6 nd ns-interval interval
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6_address</code></td>
<td>IPv6 address of the host.</td>
</tr>
<tr>
<td><code>mac_address</code></td>
<td>Layer 2 media access control (MAC) address.</td>
</tr>
</tbody>
</table>

**Command Modes**

- Interface configuration mode
- Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>ACE Module/Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A5(1.0)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The ACE stores the static neighbor entry in the ND cache.

**Examples**

To configure a static ND entry, enter the following commands:

```
host1/Admin(config)# interface vlan 100
host1/Admin(config-if)# ipv6 neighbor 2001:DB8:1::2 00-0c-f1-56-98-ad
```

To remove the static ND entry, enter the following command:

```
host1/Admin(config)# interface vlan 100
host1/Admin(config-if)# no ipv6 neighbor
```

**Related Commands**

This command has no related commands.
(config-if) ipv6 normalization

To enable TCP normalization on an IPv6 interface after it has been disabled, use the `ipv6 normalization` command. This feature is enabled by default. Use the `no` form of this command to disable TCP normalization.

```
ipv6 normalization
no ipv6 normalization
```

**Syntax Description**
This command has no keywords or arguments.

**Command Modes**
Interface configuration mode
Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>ACE Module/Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A5(1.0)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

By default, TCP normalization is enabled.

Caution
If you disable TCP normalization, you may expose your ACE and your data center to potential security risks. TCP normalization helps protect the ACE and the data center from attackers by enforcing strict security policies that are designed to examine traffic for malformed or malicious segments.

To operate your ACE for load balancing only, disable TCP normalization by entering the `no ipv6 normalization` command. You must also disable the ACE Internet Control Message Protocol (ICMP) security checks by using the `no icmp-guard` command. For details about operating your ACE as a load balancer only, see the *Server Load-Balancing Guide, Cisco ACE Application Control Engine*.

Disabling TCP normalization affects only Layer 4 traffic. TCP normalization is always enabled for Layer 7 traffic.

Use the `no ipv6 normalization` command when you encounter the following two types of asymmetric flows, which would otherwise be blocked by the normalization checks that the ACE performs:

- ACE sees only the client-to-server traffic. For example, for a TCP connection, the ACE sees the SYN from the client, but not the SYN-ACK from the server. In this case, apply the `no ipv6 normalization` command to the client-side VLAN.

- ACE sees only the server-to-client traffic. For example, for a TCP connection, the ACE receives a SYN-ACK from the server without having received the SYN from the client. In this case, apply the `no ipv6 normalization` command to the server-side VLAN.

With TCP normalization disabled, the ACE still sets up flows for the asymmetric traffic described above and makes entries in the connection table. Note that the ACE does not check the TCP flags and TCP state of the connection. If a connection is in the half-closed state and a new SYN arrives, the connection is still used but the states do not change. Once the connection is closed properly, the extra ACK from the server goes through as a routed connection and the address is not masked to originate from the VIP.
With TCP normalization enabled, when the ACE receives the final ACK, the ACE removes the entry from the connection table. Even if FIN/ACK retransmission occurs, the ACE drops this packet due to TCP normalization feature. This means that the client cannot receive the final ACK and keeps the LAST_ACK state until half-close timeout occurs by the client.

**Examples**

To enable TCP normalization after you have disabled it, enter:

```bash
host1/Admin(config)# interface vlan 200
host1/Admin(config-if)# ipv6 normalization
```

To disable TCP normalization, enter:

```bash
host1/Admin(config-if)# no ipv6 normalization
```

**Related Commands**

```
(config-if) ipv6 icmp-guard
```
(config-if) ipv6 verify reverse-path

To enable unicast reverse-path forwarding (URPF) based on the source IPv6 address for a VLAN interface, use the `ipv6 verify reverse-path` command. By default, URPF is disabled on the interface. Use the `no` form of this command to disable URPF after it has been enabled.

```
ipv6 verify reverse-path
no ipv6 verify reverse-path
```

**Syntax Description**

This command has no keywords or arguments.

**Command Modes**

Interface configuration mode

Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>ACE Module/Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A5(1.0)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

URPF helps to mitigate problems caused by the introduction of malformed or forged (spoofed) IPv6 source addresses into a network by allowing the ACE to discard IPv6 packets that lack a verifiable source IP address. This feature enables the ACE to filter both ingress and egress packets to verify addressing and route integrity. The route lookup is typically based on the destination address, not the source address.

When you enable URPF, the ACE discards packets if no route is found or if the route does not match the interface on which the packet arrived.

You cannot use this command when URPF based on the source MAC address for a VLAN interface is enabled through the (config-if) `mac-sticky enable` command.

**Examples**

To enable URPF, enter:

```
host/Admin(config-if)# ipv6 verify reverse-path
```

To disable URPF, enter:

```
host/Admin(config-if)# no ipv6 verify reverse-path
```

**Related Commands**

(config-if) `mac-sticky enable`
(config-if) mac-address autogenerate

To enable the autogeneration of a MAC address on a VLAN interface, use the `mac-address autogenerate` command. Use the `no` form of this command to disable MAC address autogeneration.

```
mac-address autogenerate

no mac-address autogenerate
```

**Syntax Description**
This command has no keywords or arguments.

**Command Modes**
Interface configuration mode

**Command History**

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A2(1.0)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(7)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
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. Thus the ACE allocates the same MAC address to them.

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

When you issue the `mac-address autogenerate` command, the ACE assigns a MAC address from the bank of MAC address for shared VLANs. If you issue 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 readd it.

**Examples**
To enable MAC address autogeneration on the VLAN, enter:

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

To disable MAC address autogeneration on the VLAN, enter:

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

**Related Commands**
This command has no related commands.
(config-if) mac-sticky enable

To enable the mac-sticky feature for a VLAN interface, use the **mac-sticky** command. 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. By default, the mac-sticky feature is disabled on the ACE. Use the **no** form of this command to disable the mac-sticky feature, resetting the default behavior of the ACE performing a route lookup to select the next hop to reach the client.

```plaintext
mac-sticky enable
no mac-sticky enable
```

**Syntax Description**
This command has no keywords or arguments.

**Command Modes**
Interface configuration mode
Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0(0)A1(2)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(7)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
When you use this command to enable the mac-sticky feature, the ACE uses the source MAC address from the first packet of a new connection to determine the device to send the return traffic. This guarantees that the ACE sends the return traffic for load-balanced connections to the same device originating the connection. By default, the ACE performs a route lookup to select the next hop to reach the client.

This feature is useful when the ACE receives traffic from Layer-2/Layer-3 adjacent stateful devices, like firewalls and transparent caches, guaranteeing that it sends return traffic to the correct stateful device that sourced the connection without any requirement for source NAT. For more information on firewall load balancing, see the *Security Guide, Cisco ACE Application Control Engine*.

You cannot use this command when RPF based on the source IP address for a VLAN interface is enabled through the **(config-if) ip verify reverse-path** command.

**Examples**
To enable the mac-sticky feature, enter:

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

To disable the mac-sticky feature, enter:

```
host/Admin(config-if)# no mac-sticky enable
```
Related Commands (config-if) ip verify reverse-path
(config-if) mtu

To specify the maximum transmission unit (MTU) for a VLAN interface, use the mtu command. This command allows you to set the data size that is sent on a connection. Use the no form of this command to reset the MTU block size to the default of 1280 (IPv6) or 1500 (IPv4) for Ethernet interfaces.

```
mtu bytes

no mtu
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mtu bytes</td>
<td>Number of bytes in the MTU. For IPv6, enter a number from 1280 to 9216 bytes. The default is 1500. For IPv4, enter a number from 64 to 9216 bytes. The default is 1500.</td>
</tr>
</tbody>
</table>

### Command Modes

Interface configuration mode

Admin and user contexts

### Command History

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0(0)A1(2)</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>A5(1.0)</td>
<td>Modified range and default for IPv6 support.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(7)</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>A5(1.0)</td>
<td>Modified range and default for IPv6 support.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The default 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 it. The ACE fragments packets that are larger than the MTU value before sending them to the next hop.

### Examples

To specify the MTU data size of for an Ethernet interface, enter the following command:

```
host1/admin(config-if)# mtu 1300
```

To reset the MTU block size to the default value of 1500 for Ethernet interfaces, enter:

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

### Related Commands

show interface
(config-if) nat-pool

To create a pool of IP addresses for dynamic Network Address Translation (NAT) for a VLAN interface, use the `nat-pool` command. Use the `no` form of this command to remove a NAT pool from the configuration.

```
  nat-pool nat_id [ipv6_address1[/prefix_length] [ipv6_address2[/prefix_length]]] [ipv4_address1 [ipv4_address2] netmask mask] [pat]

  no nat-pool nat_id ip_address1 [ip_address2] netmask mask [pat]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>nat_id</code></td>
<td>Identifier of the NAT pool of global IP addresses. Enter an integer from 1 to 2147483647.</td>
</tr>
<tr>
<td><code>ipv6_address1</code></td>
<td>Single IPv6 address and optional prefix length, or if you are also using the <code>ipv6_address2</code> argument, the first IP address in a range of global addresses used for NAT.</td>
</tr>
<tr>
<td><code>ipv6_address2</code></td>
<td>(Optional) Highest IPv6 address and optional prefix length in a range of global IPv6 addresses used for NAT. You can configure a maximum of 64 K addresses in a NAT pool.</td>
</tr>
<tr>
<td><code>ip_address1</code></td>
<td>Single IP address, or if also using the <code>ip_address2</code> argument, the first IP address in a range of global addresses used for NAT. Enter an IP address in dotted-decimal notation (for example, 172.27.16.10).</td>
</tr>
<tr>
<td><code>ip_address2</code></td>
<td>(Optional) Highest IP address in a range of global IP addresses used for NAT. Enter an IP address in dotted-decimal notation (for example, 172.27.16.109).</td>
</tr>
<tr>
<td><code>netmask</code></td>
<td>Specifies the subnet mask for the IP address pool. Enter a mask in dotted-decimal notation (for example, 255.255.255.0). If you do not specify a network mask for the global IP addresses in the pool, the ACE, by default, uses the network mask of the interface to which the pool is attached.</td>
</tr>
<tr>
<td><code>pat</code></td>
<td>(Optional) Specifies that the ACE perform Port Address Translation (PAT) in addition to NAT.</td>
</tr>
</tbody>
</table>

### Command Modes

- Interface configuration mode
  - Admin and user contexts

### Command History

#### ACE Module Release
<table>
<thead>
<tr>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Added IPv6 support.</td>
</tr>
</tbody>
</table>

#### ACE Appliance Release
<table>
<thead>
<tr>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Added IPv6 support.</td>
</tr>
</tbody>
</table>
Usage Guidelines

Dynamic NAT uses a pool of global IP addresses that you specify. You can define either a single global IP address for a group of servers with PAT to differentiate between them or a range of global IP addresses when using dynamic NAT only. To use a single IP address or a range of addresses, you assign an identifier to the address pool. You then associate the NAT pool with a global interface that is different from the interface that you use to filter and receive NAT traffic.

The ACE allows you to configure a virtual IP (VIP) address in the NAT pool for dynamic NAT and PAT. This action is useful when you want to source NAT real server originated connections (bound to the client) using the VIP address. This feature is specifically useful when there are a limited number of real world IP addresses on the client-side network. To perform PAT for different real servers that are source-NATed to the same IP address (VIP), you must configure the `pat` keyword in the `nat-pool` command.

If a packet egresses an interface that you have not configured for NAT, the ACE transmits the packet untranslated.

If the ACE runs out of IP addresses in a NAT pool, it can switch over to a PAT rule, if configured. For example, you can configure the following:

```
nat-pool 1 10.1.100.10 10.1.100.99 netmask 255.255.255.255
nat-pool 1 10.1.100.100 10.1.100.100 netmask 255.255.255.255 pat
```

Examples

**IPv6 Example**

To configure a NAT pool that consists of a range of global IPv6 addresses with PAT, enter:

```
host1/C1(config-if)# nat-pool 1 2001:DB8:1::/64 2001:DB8:1::1/64 pat
```

**IPv4 Example**

To configure a NAT pool that consists of a range of 100 global IPv4 addresses with PAT, enter:

```
host1/C1(config-if)# nat-pool 1 172.27.16.10 172.27.16.109 netmask 255.255.255.0 pat
```

Related Commands

```
show nat-fabric
(config-pmap-lb-c) nat dynamic
```

(config-if) normalization

To enable TCP normalization, use the `normalization` command. This feature is enabled by default. Use the `no` form of this command to disable TCP normalization.

```
normalization
no normalization
```

Syntax Description

This command has no keywords or arguments.

Command Modes

Interface configuration mode

Admin and user contexts
By default, TCP normalization is enabled. If you disable TCP normalization, you may expose your ACE and your data center to potential security risks. TCP normalization helps protect the ACE and the data center from attackers by enforcing strict security policies that are designed to examine traffic for malformed or malicious segments.

To operate your ACE for load balancing only, disable TCP normalization by entering the `no normalization` command. You must also disable the ACE Internet Control Message Protocol (ICMP) security checks by using the `no icmp-guard` command. For details about operating your ACE as a load balancer only, see the Server Load-Balancing Guide, Cisco ACE Application Control Engine.

Disabling TCP normalization affects only Layer 4 traffic. TCP normalization is always enabled for Layer 7 traffic. Use the `no normalization` command when you encounter the following two types of asymmetric flows, which would otherwise be blocked by the normalization checks that the ACE performs:

- ACE sees only the client-to-server traffic. For example, for a TCP connection, the ACE sees the SYN from the client, but not the SYN-ACK from the server. In this case, apply the `no normalization` command to the client-side VLAN.
- ACE sees only the server-to-client traffic. For example, for a TCP connection, the ACE receives a SYN-ACK from the server without having received the SYN from the client. In this case, apply the `no normalization` command to the server-side VLAN.

With TCP normalization disabled, the ACE still sets up flows for the asymmetric traffic described above and makes entries in the connection table. Note that the ACE does not check the TCP flags and TCP state of the connection. If a connection is in the half-closed state and a new SYN arrives, the connection is still used but the states do not change. Once the connection is closed properly, the extra ACK from the server goes through as a routed connection and the address is not masked to originate from the VIP.

With TCP normalization enabled, when the ACE receives the final ACK, the ACE removes the entry from the connection table. Even if FIN/ACK retransmission occurs, the ACE drops this packet due to TCP normalization feature. This means that the client cannot receive the final ACK and keeps the LAST_ACK state until half-close timeout occurs by the client.

To enable TCP normalization after you have disabled it, enter:

```plaintext
host1/Admin(config)# interface vlan 200
host1/Admin(config-if)# normalization
```

To disable TCP normalization, enter:

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

### Examples

- ```plaintext
   host1/Admin(config-if)# (config-if) icmp-guard
   ```

### Related Commands

- `interface vlan`
(config-if) normalization send-reset

To enable sending a RST to the peer so it can reset its TCP connections for any non-SYN packets that are a connection miss, use the `normalization send-reset` command. This feature is disabled by default. Use the `no` form of this command to disable the normalization RST function. When disabled, the ACE silently drops any non-SYN packet when there is no flow.

```
normalization send-reset
no normalization send-reset
```

**Syntax Description**
This command has no keywords or arguments.

**Command Modes**
Interface configuration mode
Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A4(1.1)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Ensure that TCP normalization is enabled through the `normalization` command and that the switch mode feature is disabled (the `switch-mode` command in configuration mode).

**Examples**
To enable sending a RST to the peer so it can reset its TCP connections for any non-SYN packets, enter:

```
host1/Admin(config)# interface vlan 200
host1/Admin(config-if)# normalization
host1/Admin(config-if)# normalization send-reset
```

To disable the normalization RST function, enter:

```
host1/Admin(config-if)# no normalization send-reset
```

**Related Commands**

```
Normal (config-if) normalization
Normal (config) switch-mode
```

**(config-if) peer ip address**

To configure the IP address of a standby ACE for the bridge-group virtual interface (BVI) or VLAN interface, use the `peer ip address` command. Use the `no` form of this command to delete the IP address of the peer ACE.

```
peer ip address {ipv6_address [prefix_length] [eui64 | link-local | unique-local]} {ipv4_address mask secondary}
```
no peer ip address {ipv6_address [/prefix_length] [eui64 | link-local | unique-local]} {ipv4_address mask [secondary]}
When you configure redundancy, configuration mode on the standby ACE is disabled by default and changes on an active ACE are automatically synchronized to the standby ACE. However, interface IP addresses on the active and standby ACEs must be unique. To ensure that the addresses on the interfaces are unique, the interface IP address on the active ACE is synchronized to the standby ACE as the peer IP address. To configure an interface IP address on the standby ACE, use the `peer ip address` command. The peer IP address on the active ACE is synchronized on the standby ACE as the interface IP address.

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

You can configure only one IPv6 peer link-local or IPv6 peer unique local address on an interface. Any additional peer link-local or peer unique local address that you configure will overwrite the existing one.

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.

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

You cannot configure secondary IPv4 addresses on FT VLANs.

**Examples**

To configure an IP address and mask for the peer ACE, enter:

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

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

```
host1/Admin(config-if)# peer ip address 12.0.0.81 255.0.0.0 secondary
```

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

```
host1/Admin(config-if)# no peer ip address 11.0.0.81 255.0.0.0
```

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

```
host1/Admin(config-if)# no peer ip address 12.0.0.81 255.0.0.0 secondary
```

**Related Commands**

`show interface`
(config-if) port-channel load-balance

(ACE appliance only) To set the load-distribution method among the ports in the EtherChannel bundle, use the **port-channel load-balance** command. Use the **no** form of the command to remove the load-distribution method.

```
port-channel load-balance { dst-ip | dst-mac | dst-port | src-dst-ip | src-dst-mac | src-dst-port |
src-ip | src-mac | src-port }
```

```
no port-channel load-balance { dst-ip | dst-mac | dst-port | src-dst-ip | src-dst-mac | src-dst-port |
src-ip | src-mac | src-port }
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dst-ip</td>
<td>Loads the distribution on the destination IP address</td>
</tr>
<tr>
<td>dst-mac</td>
<td>Loads the distribution on the destination MAC address</td>
</tr>
<tr>
<td>dst-port</td>
<td>Loads the distribution on the destination TCP or UDP port</td>
</tr>
<tr>
<td>src-dst-ip</td>
<td>Loads the distribution on the source or destination IP address</td>
</tr>
<tr>
<td>src-dst-mac</td>
<td>Loads the distribution on the source or destination MAC address</td>
</tr>
<tr>
<td>src-dst-port</td>
<td>Loads the distribution on the source or destination port</td>
</tr>
<tr>
<td>src-ip</td>
<td>Loads the distribution on the source IP address</td>
</tr>
<tr>
<td>src-mac</td>
<td>Loads the distribution on the source MAC address</td>
</tr>
<tr>
<td>src-port</td>
<td>Loads the distribution on the TCP or UDP source port</td>
</tr>
</tbody>
</table>

### Command Modes

- Interface configuration mode
- Admin context only

### Command History

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(7)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

An EtherChannel balances the traffic load across the links in the EtherChannel by reducing part of the binary pattern formed from the addresses in the frame to a numerical value that selects one of the links in the channel. EtherChannel load balancing can use MAC addresses or IP addresses, Layer 4 port numbers, source addresses, destination addresses, or both source and destination addresses.

Use the option that provides the load-balance criteria with the greatest variety in your configuration. For example, if the traffic on an EtherChannel is going to a single MAC address only and you use the destination MAC address as the basis of EtherChannel load balancing, the EtherChannel always chooses the same link in the EtherChannel.

### Examples

To configure an EtherChannel to balance the traffic load across the links using source or destination IP addresses, enter:

```
host1/Admin(config)# interface gigabitEthernet 1/1
host1/Admin(config-if)# port-channel load-balance src-dst-ip
```

### Related Commands

This command has no related commands.
Interface Configuration Mode Commands

Chapter 2 CLI Commands

(ACE appliance only) To enable Quality of Service (QoS) for a configured physical Ethernet port that is based on VLAN Class of Service (CoS) bits, use the `qos trust cos` command. Use the `no` form of the command to disable QoS for the Ethernet port.

```plaintext
qos trust cos

no qos trust cos
```

### Syntax Description
This command has no keywords or arguments.

### Command Modes
Interface configuration mode
Admin context only

### Command History

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A3(1.0)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines
QoS is configured at the physical port level. When you enable QoS on a trusted port, traffic is mapped into different ingress queues based on their VLAN CoS bits. If there are no VLAN CoS bits, or QoS is not enabled on the port (untrusted port), the traffic is then mapped into the lowest priority queue.

You can enable QoS for an Ethernet port configured for fault tolerance (see (config-if) `ft-port vlan`). In this case, heartbeat packets are always tagged with COS bits set to 7 (a weight of High). We recommend that you enable QoS on the FT VLAN port to provide higher priority for FT traffic.

QoS is configurable only for a physical Ethernet port and is not VLAN interface-based.

### Examples
To enable QoS for Ethernet port 3, enter:

```
host1/Admin(config)# interface gigabitEthernet 1/3
host1/Admin(config-if)# qos trust cos
```

To disable QoS for the Ethernet port, enter:

```
host1/Admin(config-if)# no qos trust cos
```

### Related Commands
`show interface`
(config-if) remove-eth-pad

To enable an internal length check and remove a trailing byte appended to the end of an Ethernet IP packet coming into the ACE, use the `remove-eth-pad` command. This check is performed on the VLAN interface and is disabled by default. Use the `no` form of the command to disable an internal length check and the removal of the trailing byte.

```
remove-eth-pad

no remove-eth-pad
```

**Syntax Description**

This command has no keywords or arguments.

**Command Modes**

Interface configuration mode

Admin context only

**Command History**

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A2(1.6)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A3(2.3)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command has no usage guidelines.

**Examples**

To enable an internal length check and remove the trailing byte appended to the end of an Ethernet IP packet coming into the ACE, enter:

```
host1/Admin(config)# interface vlan 3
host1/Admin(config-if)# remove-eth-pad
```

To disable an internal length check and the removal of the trailing byte, enter:

```
host1/Admin(config-if)# no remove-eth-pad
```

**Related Commands**

`show interface`
(config-if) service-policy input

To apply a previously created policy map and attach the traffic policy to the input direction of a VLAN interface, use the `service-policy input` command. Use the `no` form of this command to remove a service policy.

```
service-policy input policy_name

no service-policy input policy_name
```

**Syntax Description**

| policy_name | Name of a previously defined policy map, configured with a previously created `policy-map` command. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters. |

**Command Modes**

- Interface configuration mode
- Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0(0)A1(2)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(7)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When you enter the `service-policy` command in configuration mode, the policy maps that are applied globally in a context are applied on all interfaces that exist in the context. A policy activated on an interface overwrites any specified global policies for overlapping classifications and actions. The ACE allows only one policy of a specific feature type to be activated on a given interface.

**Examples**

To apply the L4SLBPOLICY policy map to an interface, enter:

```
host1/C1(config-if)# service-policy input L4SLBPOLICY
```

To remove the L4SLBPOLICY policy map from the interface, enter:

```
host1/C1(config-if)# no service-policy input L4SLBPOLICY
```

**Related Commands**

- `show service-policy`
- `(config) service-policy`
(config-if) shutdown

To disable a bridge-group virtual interface (BVI) or VLAN interface, use the `shutdown` command. Use the `no` form of this command to enable the interface.

```
shutdown
no shutdown
```

**Syntax Description**

This command has no keywords or arguments.

**Command Modes**

Interface configuration mode
Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0(0)A1(2)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

To enable a bridge-group virtual interface (BVI), VLAN interface, VLAN trunking, or for an ACE Appliance, Ethernet port or port-channel interface, use the `no shutdown` command in interface configuration mode. This puts the interface in the Up administrative state.

To disable a bridge-group virtual interface (BVI), VLAN interface, VLAN trunking, or for an ACE Appliance, Ethernet port or port-channel interface, use the `shutdown` command in interface configuration mode. This puts the interface in the Down administrative state.

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.

**Examples**

To disable an interface, enter:

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

To enable an interface for use, enter:

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

- show interface
- show running-config
(config-if) speed

(ACE appliance only) To configure the Ethernet port speed for a setting of 10, 100, or 1000 Mbps, use the speed command in interface configuration mode. The default speed for an ACE interface is autonegotiate. Use the no form of the command to return to the default Ethernet port speed setting.

```plaintext
speed {1000M | 100M | 10M | auto}
no speed
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000M</td>
<td>Initiates 1000-Mbps operation.</td>
</tr>
<tr>
<td>100M</td>
<td>Initiates 100-Mbps operation.</td>
</tr>
<tr>
<td>10M</td>
<td>Initiates 10-Mbps operation.</td>
</tr>
<tr>
<td>auto</td>
<td>Enables the ACE to autonegotiate with other devices for speeds of 10, 100, or 1000 Mbps. If you set the Ethernet port speed to auto, the ACE automatically sets the duplex mode to auto. This is the default setting.</td>
</tr>
</tbody>
</table>

**Command Modes**

Interface configuration mode
Admin context only

**Command History**

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(7)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

By default, the ACE automatically uses the autonegotiate setting for Ethernet port speed and duplex mode parameters to allow the ACE to negotiate the speed and duplex mode between ports. If you manually configure the port speed and duplex modes, follow these guidelines:

- The ACE prevents you from making a duplex setting when you configure the speed of an Ethernet port to auto. The speed command must be a non-auto setting of 10, 100, or 1000 Mbps to be able to configure the duplex setting for the Ethernet port.

- If you configure an Ethernet port speed to a value other than auto (for example, 10, 100, or 1000 Mbps), ensure that you configure the connecting port to match. Do not configure the connecting port to negotiate the speed through the auto keyword.

- The ports on both ends of a link must have the same setting. The link will not come up if the port at each end of the connecting interface has a different setting.

- If you enter the no speed command, the ACE automatically configures both the speed and duplex settings to auto.

The ACE cannot automatically negotiate interface speed and duplex mode if you configure the connecting interface to a value other than auto.

If you configure the Ethernet port speed to auto, the ACE automatically sets the duplex mode to auto.
Examples

To set the speed to 1000 Mbps on Ethernet port 3, enter:

host1/Admin(config)# interface gigabitEthernet 1/3
host1/Admin(config-if)# speed 1000M

To restore the default setting of autonegotiate for an Ethernet port, enter:

host1/Admin(config-if)# no speed

Related Commands

(config-if) duplex
(config-if) switchport access vlan

(ACE appliance only) To configure an access port to a specific VLAN for either an Ethernet interface or a Layer 2 EtherChannel interface, use the `switchport access vlan` command in interface configuration mode. Use the `no` form of the command to reset the access mode to the default VLAN 1.

```
switchport access vlan number
no switchport access vlan number
```

**Syntax Description**

- `number` VLAN number that you want to configure as the IEEE 802.1Q native VLAN when operating in trunking mode. Valid values are from 1 to 4094. The default is VLAN 1.

**Command Modes**

- Interface configuration mode
- Admin context only

**Command History**

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(7)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

On the ACE, ports are assigned to a single VLAN. These ports are referred to as access ports and provide a connection for end users or node devices, such as a router or server. By default, all devices are assigned to VLAN 1, known as the default VLAN.

You can configure a trunk on a single Ethernet port or on a port-channel interface (EtherChannel).

It is not necessary to create a VLAN interface before configuring an access VLAN. To configure a VLAN interface and access its mode to configure its attributes, use the `interface vlan` command in configuration mode for the context.

When you assign a VLAN as the access port for a specific Ethernet port or port-channel interface, the VLAN is reserved and cannot be configured as a VLAN trunk. A VLAN access port and a VLAN trunk cannot coexist for the same Ethernet port or port-channel interface. If you specify both configurations for the same Ethernet port or port-channel interface, the most recent configuration will overwrite the older configuration.

If you have QoS enabled for a physical Ethernet port (see the “(config-if) qos trust cos” command) that has been designated as an FT VLAN port (see the “(config-if) ft-port vlan” command), do not configure this Ethernet port as a VLAN access port. In this configuration, the QoS setting for redundancy traffic, such as heartbeat packets or TCP tracking probes, may not be handled properly by the ACE and FT traffic may be dropped when there is network congestion.

**Examples**

To configure VLAN 101 as an access port for Ethernet port 4, enter:
```
host1/Admin(config)# interface gigabitEthernet 1/4
host1/Admin(config-if)# switchport access vlan 101
```

To configure VLAN 101 as an access port for EtherChannel 255, enter:
```
host1/Admin(config)# interface port-channel 255
host1/Admin(config-if)# switchport access vlan 101
```
To reset the access mode to the default VLAN 1, enter:

```
host1/Admin(config)# interface gigabitEthernet 1/4
host1/Admin(config-if)# no switchport access vlan 101
```
(config-if) switchport trunk allowed vlan

(ACE appliance only) To specify which VLANs are to be allocated to a trunk link, use the switchport trunk allowed vlan command in interface configuration mode. To remove a VLAN from the trunk link, use the no form of the command.

```
switchport trunk allowed vlan vlan_list
no switchport trunk allowed vlan vlan_list
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan_list</td>
<td>The allowed VLANs that transmit this interface in tagged format when in trunking mode. The vlan_list argument can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Single VLAN number</td>
</tr>
<tr>
<td></td>
<td>• Range of VLAN numbers separated by a hyphen</td>
</tr>
<tr>
<td></td>
<td>• Specific VLAN numbers separated by commas</td>
</tr>
</tbody>
</table>

Valid entries are 1 through 4094. Do not enter any spaces between the dash-specified ranges or the comma-separated numbers in the vlan_list argument.

**Command Modes**

Interface configuration mode
Admin context only

**Command History**

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(7)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You cannot remove VLAN 1. If you remove VLAN 1 from a trunk, the trunk interface continues to send and receive management traffic in VLAN 1.

You can selectively allocate individual VLANs to a trunk link. All added VLANs are active on a trunk link, and as long as the VLAN is available for use, traffic for that VLAN is carried across the trunk link.

It is not necessary to create a VLAN interface before you allocate a VLAN to an Ethernet port or port-channel interface (EtherChannel). To configure a VLAN interface and access its mode to configure its attributes, use the interface vlan command in configuration mode for the context.

If you configure a VLAN on a trunk, you cannot configure the VLAN as the access port for a specific Ethernet port or port-channel interface. A VLAN access port and a VLAN trunk cannot coexist for the same Ethernet port or port-channel interface. If you specify both configurations for the same Ethernet port or port-channel interface, the most recent configuration will overwrite the older configuration.

When allocating VLANs to ports, overlapping is not allowed. For example, if you associate VLAN 10 with Ethernet port 1, you cannot associate VLAN 10 with another Ethernet port.

If you have QoS enabled for a physical Ethernet port (see the “(config-if) qos trust cos” command) that has been designated as an FT VLAN port (see the “(config-if) ft-port vlan” command), do not configure the FT VLAN as an 802.1Q native VLAN. In this configuration, the QoS setting for redundancy traffic, such as heartbeat packets or TCP tracking probes, may not be handled properly by the ACE and FT traffic may be dropped when there is network congestion.
Examples

To add VLANs 101, 201, and 250 through 260 to the defined list of VLANs currently set for Ethernet port 4, enter:

```
host1/Admin(config)# interface gigabitEthernet 1/4
host1/Admin(config-if)# switchport trunk allowed vlan 101,201,250-260
```

To remove VLANs 101 through 499 from the defined list of VLANs currently set for Ethernet port 4, enter:

```
host1/Admin(config)# interface gigabitEthernet 1/4
host1/Admin(config-if)# no switchport trunk allowed vlan 101-499
```
(config-if) switchport trunk native vlan

(ACE appliance only) To set the IEEE 802.1Q native VLAN for a trunk, use the switchport trunk native vlan command in interface configuration mode. Use the no form of the command to revert to the default of VLAN 1.

```
switchport trunk native vlan number

no switchport trunk native vlan number
```

**Syntax Description**
- `number`: VLAN number that you want to configure as the 802.1Q native VLAN when operating in trunking mode. Valid values are from 1 to 4094. The default is VLAN 1.

**Command Modes**
- Interface configuration mode
- Admin context only

**Command History**

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(7)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You can only have one assigned native VLAN.

The native VLAN is the VLAN that is assigned to all ports in the ACE. By default, all interfaces are in VLAN 1 on the ACE, and VLAN 1 is the native VLAN. Depending on your network needs, you may change the native VLAN to be other than VLAN 1.

When configuring 802.1Q trunking, you must match the native VLAN across the link. Because the native VLAN is untagged, you must keep the native VLAN the same on each side of the trunk line. The native VLAN must match on both sides of the trunk link for 802.1Q; otherwise, the link will not work.

It is not necessary to create a VLAN interface setting the 802.1Q native VLAN for a trunk. To configure a VLAN interface and access its mode to configure its attributes, use the `interface vlan` command in configuration mode for the context.

**Examples**

To specify VLAN 3 as the 802.1Q native VLAN for the trunk, enter:

```
host1/Admin(config)# interface port-channel 255
host1/Admin(config-if)# switchport trunk native vlan 3
```

To revert to the default of VLAN 1, enter:

```
host1/Admin(config-if)# no switchport trunk native vlan
```

**Related Commands**
- (config) interface
(config-if) syn-cookie

To configure SYN-cookie-based DoS protection, use the `syn-cookie` command. Use the `no` form of this command to remove SYN-cookie DoS protection from the interface.

```
syn-cookie number

no syn-cookie
```

**Syntax Description**

- `number` Embryonic connection threshold above which the ACE applies SYN-cookie DoS protection. Enter an integer from 1 to 65535.

**Command Modes**

- Interface configuration mode
- Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A2(1.0)</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>A4(1.0)</td>
<td>The embryonic connection threshold range changed to 1 to 65535 (from 2 to 65535).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A3(1.0)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Keep in mind the following guidelines when you use the SYN cookie feature:

- If the server drops the SYN that is sent by the ACE, the ACE resets the connection using the embryonic timeout. It does not retry the SYN packet.
- A SYN cookie supports only the MSS TCP option. The ACE ignores all other TCP options, even if there are problems with those other options.
- The ACE returns an MSS of 536 to the client, which is the RFC-specified default.
- If you use a parameter map to specify the minimum and maximum MSS values, the ACE ignores those values.
- Disabling normalization and using a SYN cookie concurrently may result in unpredictable behavior.
- The ACE does not generate any syslogs for a SYN cookie, even if the number of embryonic connections exceeds the configured threshold, which may indicate a SYN-flood attack.
- (ACE module only) When you configure SYN cookie protection, the ACE calculates the internal embryonic connection threshold value for each network processor (NP) as `configured_threshold ÷ 4` (fractions are not disregarded). For example, if you configure the threshold as 6, the ACE applies the threshold to each NP in a round-robin fashion in the order shown, which results in the following threshold distribution:
  - NP1=2
  - NP2=2
Because of this internal division of the threshold value, you may occasionally observe that SYN cookie protection is applied before the embryonic connection count reaches the configured threshold value. For example, suppose that you configure a threshold value of 4. Because the threshold value is divided by four internally for each NP, the internally calculated threshold is 1. After one incomplete connection attempt (SYN) is sent to an NP, the ACE activates SYN cookie protection and intercepts the second SYN going to that same NP.

- If you are configuring the SYN cookie feature on a bridged VLAN with non-loadbalanced flows, you must configure static routes for non-loadbalanced destinations that do not reside in the same subnet as the bridge-group virtual interface (BVI).

### IPv6 Configuration

For example, assuming the following IPv6 configuration:

- BVI IPv6 address is 2001:DB8:1::1
- Gateway1 IPv6 address 2001:DB8:1::2 to reach external network 2001:DB8:2::1
- Gateway2 IPv6 address 2001:DB8:1::3 to reach external network 2001:DB8:3::1

Configure the following static routes:

- `ip route 2001:DB8:2::1/64 2001:DB8:1::2`
- `ip route 2001:DB8:3::1/64 2001:DB8:1::3`

### IPv4 Configuration

For example, assuming the following IPv4 configuration:

- BVI IPv4 address is 192.168.1.1
- Gateway1 IPv4 address 192.168.1.2 to reach external network 172.16.1.0
- Gateway2 IPv4 address 192.168.1.3 to reach external network 172.31.1.0

Configure the following static routes:

- `ip route 172.16.1.0 255.255.255.0 192.168.1.2`
- `ip route 172.31.1.0 255.255.255.0 192.168.1.3`

### Examples

To configure SYN-cookie DoS protection for servers in a data center connected to VLAN 100, enter:

```bash
host1/C1(config)# interface vlan 100
host1/C1(config-if)# syn-cookie 4096
```

To remove SYN-cookie DoS protection from the interface, enter:

```bash
host1/C1(config-if)# no syn-cookie
```

### Related Commands

- `show interface`
- `show running-config`
(config-if) udp

To enable the UDP booster feature for applications that require very high UDP connection rates, use the `udp` command in interface configuration mode. The syntax of this command is as follows:

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

```
no udp
```

### Syntax Description

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-source-hash</td>
<td>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.</td>
</tr>
<tr>
<td>ip-destination-hash</td>
<td>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.</td>
</tr>
</tbody>
</table>

### Command Modes

Interface configuration mode

Admin and user contexts

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACE Module</td>
<td></td>
</tr>
<tr>
<td>A2(1.0)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACE Appliance</td>
<td></td>
</tr>
<tr>
<td>A3(1.0)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

For the UDP booster feature to work, you must configure both command keywords on their respective interfaces.

Do not configure this feature with NAT or with any Layer 7 feature, for example, per-packet UDP load balancing (also called UDP fast-age) using the `loadbalance vip udp-fast-age` command. Otherwise, unexpected results may occur.

For detailed information concerning this feature and its configuration, see the Server Load-Balancing Guide, Cisco ACE Application Control Engine.

### Examples

To configure the UDP booster feature on the client VLAN 100, enter:

```
host1/C1(config)# interface vlan 100
host1/C1(config-if)# udp ip-source-hash
```

To configure the UDP booster feature on the server VLAN 200, enter:

```
host1/C1(config)# interface vlan 200
host1/C1(config-if)# udp ip-destination-hash
```

To remove the UDP booster feature from an interface, enter:
host1/C1(config-if)# no udp

**Related Commands**
- show interface
- show running-config