

Interface Configuration Mode Commands

Interface configuration mode commands allow you to configure a VLAN interface, a bridge-group virtual interface (BVI), 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 <i>group_number</i>	Creates a BVI for a bridge group and accesses interface configuration mode commands for the BVI. The <i>group_number</i> argument is the bridge-group number configured on a VLAN interface.
gigabitEthernet <i>slot_number/</i> <i>port_number</i>	Specifies one of the four Ethernet ports on the rear panel of the ACE. <ul style="list-style-type: none"> <i>slot_number</i>—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. <i>port_number</i>—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 <i>channel_number</i>	Specifies the channel number assigned to this port-channel interface. Valid values are from 1 to 255.
vlan <i>number</i>	Assigns the VLAN to the context and accesses interface configuration mode commands for the VLAN. The <i>number</i> argument is the number for a VLAN assigned to the ACE.

Command Modes

Configuration mode
 BVI and VLAN interface—Admin and user contexts
 Ethernet port and port-channel interface—Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the interface feature in your user role. In addition, the Ethernet port and port-channel interface command functions require the Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

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.

The ACE supports a maximum of 4,093 VLAN interfaces with a maximum of 1,024 shared VLANs.

The ACE supports a maximum of 4,094 BVI interfaces.

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

Examples

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

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

To remove a VLAN, enter:

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

To create a BVI for bridge group 15, enter:

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

To delete a BVI for bridge group 15, enter:

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

Related Commands

[show arp](#)
[show interface](#)
[show ip](#)
[show running-config](#)
[show vlans](#)

(config-if) access-group

To apply an 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.
	<i>acl_name</i>	Identifier of an existing ACL that you want to apply to an interface.

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

Command History	Release	Modification
	A1(7)	This command was introduced.

Usage Guidelines

You must apply ACLs to a VLAN interface to allow the traffic to pass on an interface. You can apply one 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

- [show access-list](#)
- [\(config\) access-group](#)
- [\(config\) access-list extended](#)

(config-if) alias

To configure an IP address that is shared between active and standby appliances 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 ip_address mask
```

```
no alias ip_address mask
```

Syntax Description		
<i>ip_address</i>		IP address of the interface. Enter the IP address in dotted-decimal notation (for example, 172.16.27.1).
<i>mask</i>		Subnet mask of the interface. Enter the subnet mask in dotted-decimal notation (for example, 255.255.255.0).

Command Modes	
	Interface configuration mode Admin and user contexts

Command History	Release	Modification
	A1(7)	This command was introduced.

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 *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

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

Examples

To configure an alias IP address and mask, enter:

```
host1/Admin(config)# interface vlan 2
host1/Admin(config-if)# alias 12.0.0.81 255.0.0.0
```

To delete the alias IP address, enter:

```
host1/Admin(config-if)# no alias 12.0.0.81 255.0.0.0
```

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.

```
arp ip_address mac_address
```

```
no arp ip_address mac_address
```

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

Command Modes	
	Interface configuration mode Admin and user contexts

Command History	Release	Modification
	A1(7)	This command was introduced.

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 the following command: <pre>host1/Admin(config)# interface vlan 2 host1/Admin(config-if)# arp 10.1.1.1 00.02.9a.3b.94.d9</pre>
	To remove a static ARP entry, use the no arp command. For example, enter: <pre>host1/Admin(config-if)# no arp 10.1.1.1 00.02.9a.3b.94.d9</pre>

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	<i>number</i>	Bridge-group number. Enter an integer from 1 to 4094.
---------------------------	---------------	---

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

Command History	Release	Modification
	A1(7)	This command was introduced.

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 a VLAN, enter:

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

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	<i>channel_number</i>	Channel number assigned to this channel group. Valid values are from 1 to 255.
--------------------	-----------------------	--

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

Command History	Release	Modification
	A1(7)	This command was introduced.

Usage Guidelines	<p>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.</p> <p>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.</p>
------------------	--

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 VLAN interface, a bridge-group virtual interface (BVI), an Ethernet port or a port-channel interface, use the **description** command. Use the **no** form of this command to delete the description.

description *text*

no description

Syntax Description

<i>text</i>	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

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To provide a description for a VLAN interface, enter:

```
host1/Admin(config)# interface vlan 200
host1/admin(config-if)# description FOR INBOUND AND OUTBOUND TRAFFIC
```

To provide a description for Ethernet port 1, enter:

```
host1/Admin(config)# interface gigabitEthernet 1/3
host1/Admin(config-if)# description Ethernet port 3 is configured for speeds of 1000 Mbps
```

To remove the description for the interface, enter:

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

Related Commands

[show interface](#)

(config-if) duplex

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

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

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

Command History	Release	Modification
	A1(7)	This command was introduced.

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: <pre>host1/Admin(config)# interface gigabitEthernet 1/3 host1/Admin(config-if)# duplex full</pre> To restore the default setting of autonegotiate for an Ethernet port, enter: <pre>host1/Admin(config-if)# no duplex</pre>
----------	--

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 for this command to reset the default value.

fragment chain *number*

no fragment chain

Syntax Description	<i>number</i>	Maximum number of fragments that belong to the same packet. Enter an integer from 1 to 256. The default is 24.
---------------------------	---------------	--

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

Command History	Release	Modification
	A1(7)	This command was introduced.

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

Examples To configure a fragment chain limit of 126, enter:

```
host1/Admin(config)# interface vlan 200
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 for this command to reset the default value.

fragment min-mtu *number*

no fragment min-mtu

Syntax Description	<i>number</i>	Minimum fragment size. Enter an integer from 68 to 9216 bytes. The default is 576 bytes.
--------------------	---------------	--

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

Command History	Release	Modification
	A1(7)	This command was introduced.

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

Examples To configure a minimum fragment size of 1024, enter:

```
host1/Admin(config)# interface vlan 200
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 for this command to reset the default value.

fragment timeout *seconds*

no fragment timeout

Syntax Description

<i>seconds</i>	Reassembly timeout in seconds. Enter an integer from 0 to 65535. A value of 0 instructs the ACE to never time out. The default is 10.
----------------	---

Command Modes

Interface configuration mode
Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

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 750 seconds, enter:

```
host1/Admin(config)# interface vlan 200
host1/C1(config-if)# fragment timeout 750
```

To reset the fragment timeout to the default value of 10 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

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	<i>number</i>	Unique identifier for the FT VLAN. Valid values are from 2 to 4094.
---------------------------	---------------	---

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

Command History	Release	Modification
	A1(7)	This command was introduced.

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.

You cannot use this dedicated FT VLAN Ethernet port for normal network traffic; it must be dedicated for redundancy only.

When you specify an Ethernet port or a port-channel interface as a dedicated FT VLAN, you have the option to either configure the dedicated VLAN as the only VLAN associated with the Ethernet port or port-channel interface, or to allocate it as part of a VLAN trunk link (see “(config-if) [switchport trunk allowed vlan](#)”). Note that the ACE automatically includes the FT VLAN in the VLAN trunk link. If you choose to configure VLAN trunking, it is not necessary for you to assign the FT VLAN in the trunk link along with the other VLANs.

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

For details on configuring redundant ACE appliances, including an FT VLAN, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

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
-------------------------	--------------------------------

(config-if) icmp-guard

To enable the ICMP security checks in the ACE, 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	Release	Modification
	A1(7)	This command was introduced.

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

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

ip address *ip_address mask*

no ip address

Syntax Description		
<i>address</i>		IP address and mask for the interface. Enter an IP address in dotted-decimal notation (for example, 192.168.12.1).
<i>mask</i>		Subnet mask of the interface. Enter the subnet mask in dotted-decimal notation (for example, 255.255.255.0).

Command Modes	
	Interface configuration mode
	Admin and user contexts

Command History	Release	Modification
	A1(7)	This command was introduced.

Usage Guidelines	
	When you assign an IP address to an interface, the ACE automatically makes the interface routed. 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.

Examples To set the IP address of 192.168.1.1 255.255.255.0 for VLAN interface 200, enter:

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

To remove the IP address for the VLAN, enter:

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

Related Commands	
	show arp
	show interface
	show ip

(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	clear	allow
	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.	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.

Command Modes
Interface configuration mode
Admin and user contexts

Command History	Release	Modification
	A1(7)	This command was introduced.

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)# interface vlan 200
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	Release	Modification
	A1(7)	This command was introduced.

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)# interface vlan 200
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

<i>ip_address</i>	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

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

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

```
host1/Admin(config)# interface vlan 200
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 the command to instruct the ACE to ignore the IP option.

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

no ip options

Syntax Description		
allow		Allows the packet with the IP options set.
clear		Clears the specified option from the packet and allows the packet.
clear-invalid		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.
drop		Causes the ACE to discard the packet.

Command Modes	
	Interface configuration mode Admin and user contexts

Command History	Release	Modification
	A1(7)	This command was introduced.

Usage Guidelines	
	This command has no usage guidelines.

Examples	
	To allow packets with IP options set, enter: <pre>host1/Admin(config)# interface vlan 200 host1/Admin(config-if)# ip options allow</pre>
	To reset the ACE to its default of clearing all IP options if the appliance encounters one or more invalid or unsupported IP options, enter: <pre>host1/Admin(config-if)# no ip options</pre>

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	<i>number</i>	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	Release	Modification
	A1(7)	This command was introduced.

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 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.
------------------	--

Examples	To set the TTL hops to 15, enter: <pre>host1/Admin(config)# interface vlan 200 host1/Admin(config-if)# ip ttl minimum 15</pre>
----------	---

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	Release	Modification
	A1(7)	This command was introduced.

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:

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

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	Release	Modification
	A1(7)	This command was introduced.

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 *Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*.

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 1500 for Ethernet interfaces.

mtu *bytes*

no mtu

Syntax Description	<i>bytes</i>	Number of bytes in the MTU; valid values are from 64 to 9216 bytes. The default is 1500.
---------------------------	--------------	--

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

Command History	Release	Modification
	A1(7)	This command was introduced.

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 1000 for an interface, enter:

```
host1/Admin(config)# interface vlan 200
host1/admin(config-if)# mtu 1000
```

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 ip_address1 [ip_address2] netmask mask [pat]
```

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

Syntax Description

<i>nat_id</i>	Identifier of the NAT pool of global IP addresses. Enter an integer from 1 to 2147483647.
<i>ip_address1</i>	Single IP address, or if also using the <i>ip_address2</i> 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).
<i>ip_address2</i>	(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).
netmask mask	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.
pat	(Optional) Specifies that the ACE perform Port Address Translation (PAT) in addition to NAT.

Command Modes

Interface configuration mode
Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

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.

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

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

```
host1/Admin(config)# interface vlan 200  
host1/C1(config-if)# nat-pool 1 172.27.16.10 172.27.16.109 netmask 255.255.255.0 pat
```

Related Commands

This command has no related commands.

(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

Command History

Release	Modification
A1(7)	This command was introduced.

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

Examples

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

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

To disable TCP normalization, enter:

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

Related Commands

[\(config-if\) icmp-guard](#)

(config-if) peer ip address

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

peer ip address *ip_address mask*

no peer ip address

Syntax Description		
<i>ip_address</i>		IP address of the peer appliance. Enter the address in dotted-decimal IP notation (for example, 192.168.11.1).
<i>mask</i>		Subnet mask of the peer appliance. Enter the subnet mask in dotted-decimal notation (for example, 255.255.255.0).

Command Modes	
	Interface configuration mode for BVI and VLAN interfaces Admin and user contexts

Command History	Release	Modification
	A1(7)	This command was introduced.

Usage Guidelines

When you configure redundancy, configuration mode on the standby appliance is disabled by default and changes on an active appliance are automatically synchronized on the standby appliance. However, interface IP addresses on the active and standby appliances must be unique. To ensure that the addresses on the interfaces are unique, the interface IP address on the active appliance is synchronized on the standby appliance as the peer IP address. To configure an interface IP address on the standby appliance, use the **peer ip address** command. The peer IP address on the active appliance is synchronized on the standby appliance 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.

Examples

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

```
host1/Admin(config)# interface vlan 200
host1/Admin(config-if)# peer ip address 11.0.0.81 255.0.0.0
```

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

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

Related Commands [show interface](#)

(config-if) port-channel load-balance

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	Parameter	Description
	dst-ip	Loads the distribution on the destination IP address
	dst-mac	Loads the distribution on the destination MAC address
	dst-port	Loads the distribution on the destination TCP or UDP port
	src-dst-ip	Loads the distribution on the source or destination IP address
	src-dst-mac	Loads the distribution on the source or destination MAC address
	src-dst-port	Loads the distribution on the source or destination port
	src-ip	Loads the distribution on the source IP address
	src-mac	Loads the distribution on the source MAC address
	src-port	Loads the distribution on the TCP or UDP source port

Command Modes	Mode
	Interface configuration mode Admin context only

Command History	Release	Modification
	A1(7)	This command was introduced.

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.

(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

<i>policy_name</i>	Name of a previously defined policy map, configured with a previously created policy-map command. Enter a text string with a maximum of 64 alphanumeric characters.
--------------------	--

Command Modes

Interface configuration mode
Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

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/Admin(config)# interface vlan 200
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), Ethernet port, port-channel interface, VLAN interface, or VLAN trunking, 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

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

When you create an interface, the interface is in the shutdown state (administratively down) 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), Ethernet port, port-channel interface, VLAN interface, or VLAN trunking, 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), Ethernet port, port-channel interface, VLAN interface, or VLAN trunking, use the **shutdown** command in interface configuration mode. This puts the interface in the Down administrative state.

Usage Guidelines

To enable Ethernet port 3, enter:

```
host1/Admin(config)# interface gigabitEthernet 1/3
host1/Admin(config-if)# no shutdown
```

To disable Ethernet port 3, enter:

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

To enable a VLAN interface, enter:

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

To disable a VLAN interface, enter:

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

To enable VLAN trunking for Ethernet port 4, enter:

```
host1/Admin(config)# interface gigabitEthernet 1/4  
host1/Admin(config-if)# switchport trunk allowed vlan 101,201,250-260  
host1/Admin(config-if)# no shutdown
```

To disable VLAN trunking for an interface, enter:

```
host1/Admin(config-if)# switchport trunk allowed vlan 101,201,250-260  
host1/Admin(config-if)# shutdown
```

Related Commands

[show interface](#)
[show running-config](#)

(config-if) speed

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.

```
speed {1000M | 100M | 10M | auto}
```

```
no speed
```

Syntax Description		
	1000M	Initiates 1000-Mbps operation.
	100M	Initiates 100-Mbps operation.
	10M	Initiates 10-Mbps operation.
	auto	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.

Command Modes	
	Interface configuration mode
	Admin context only

Command History	Release	Modification
	A1(7)	This command was introduced.

Usage Guidelines	
	<p>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:</p> <ul style="list-style-type: none"> • 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

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	<i>number</i>	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	Release	Modification
	A1(7)	This command was introduced.

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.

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
```

Related Commands [\(config\) interface](#)

(config-if) switchport trunk allowed vlan

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	<i>vlan_list</i>	<p>The allowed VLANs that transmit this interface in tagged format when in trunking mode. The <i>vlan_list</i> argument can be one of the following:</p> <ul style="list-style-type: none"> • Single VLAN number • Range of VLAN numbers separated by a hyphen • Specific VLAN numbers separated by commas <p>Valid entries are 1 through 4094. Do not enter any spaces between the dash-specified ranges or the comma-separated numbers in the <i>vlan_list</i> argument.</p>
---------------------------	------------------	---

Command Modes	<p>Interface configuration mode</p> <p>Admin context only</p>
----------------------	---

Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>A1(7)</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	A1(7)	This command was introduced.
Release	Modification				
A1(7)	This command was introduced.				

Usage Guidelines	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>When you specify an Ethernet port or a port-channel interface as a dedicated FT VLAN (see “(config-if) ft-port vlan”) and you allocate it as part of a VLAN trunk link, the ACE automatically includes the FT VLAN in the VLAN trunk link. It is not necessary to assign the FT VLAN in the trunk link along with the other VLANs.</p>
-------------------------	--

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
```

Related Commands

[\(config\) interface](#)

(config-if) switchport trunk native vlan

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	<i>number</i>
	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	Release	Modification
	A1(7)	This command was introduced.

Usage Guidelines	<p>You can only have one assigned native VLAN.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>When you specify an Ethernet port as a dedicated FT VLAN (see “(config-if) ft-port vlan”), the ACE automatically includes the FT VLAN in the VLAN trunk link and assigns the FT VLAN as the 802.1Q native VLAN for the trunk. The ACE prevents you from selecting a different VLAN as the native VLAN.</p>
------------------	---

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
------------------	------------------------------------