CHAPTER 8

Configuring Network Access

The ACE appliance has four physical Ethernet interface ports. All VLANs are allocated to the physical ports. After the VLANs are assigned, you can configure the corresponding VLAN interfaces as either routed or bridged for use. When you configure an IP address on an interface, the ACE appliance automatically makes it a routed mode interface.

Similarly, when you configure a bridge group on an interface VLAN, the ACE appliance automatically makes it a bridged interface. Then, you associate a bridge-group virtual interface (BVI) with the bridge group.

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

In routed mode, the ACE is considered a router hop in the network. In the Admin or user contexts, the ACE supports static routes only. The ACE supports up to eight equal cost routes for load balancing.

Note When you use the ACE CLI to configure named objects (such as a real server, virtual server, parameter map, class map, health probe, and so on), consider that the Device Manager (DM) supports object names with an alphanumeric string of 1 to 64 characters, which can include the following special characters: underscore (_), hyphen (-), dot (.), and asterisk (*). Spaces are not allowed.

If you use the ACE CLI to configure a named object with special characters that the DM does not support, you may not be able to configure the ACE using DM.

Related Topics

- Configuring Port Channel Interfaces, page 8-2
- Configuring Gigabit Ethernet Interfaces, page 8-4
- Configuring Virtual Context VLAN Interfaces, page 8-8
- Configuring VLAN Interface Options, page 8-14
- Configuring Virtual Context BVI Interfaces, page 8-19
- Configuring Virtual Context Static Routes, page 8-22
- Configuring Global IP DHCP, page 8-23

Configuring Port Channel Interfaces

This section discusses how to configure port channel interfaces for the ACE appliance. It consists of the following topics:

Why Use Port Channels?

A port channel groups multiple physical ports into a single logical port. This is also called “port aggregation” or “channel aggregation.” A port channel containing multiple physical ports has several advantages:

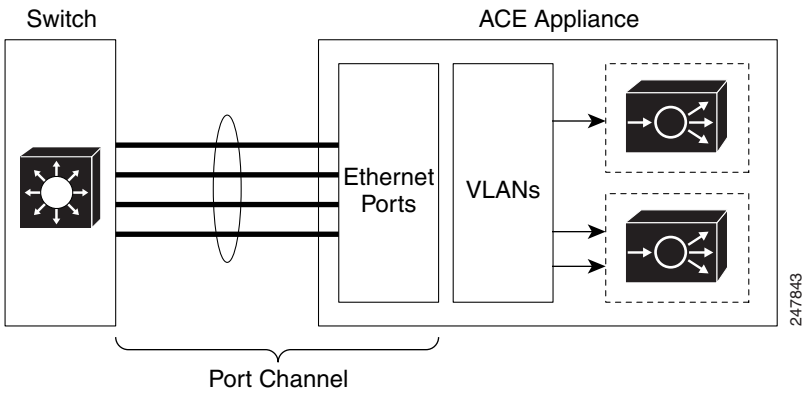
- Improves link reliability through physical redundancy.
- Allows greater total throughput to the ACE appliance. For example, four 1-GigaBit Ethernet interfaces can be aggregated into a single 4 GigaBit channel.
- Allows traffic capacity to be scaled up in the future, without network disruption at that time. A port channel can do everything a switched port can do, but a switched port cannot do everything a port channel can do. We recommend that you use a port channel.)
- Provides maximum flexibility of network configuration and focuses network configuration on VLANs rather than physical cabling

The disadvantage of a port channel is that it requires additional configuration on the switch the ACE is connected to, as well as the ACE itself. There are many methods of port aggregation implemented by different switches, and not every method works with ACE.

Using a port channel also requires more detailed knowledge of your network's VLANs, because all “cabling” to and from the ACE will be handled over VLANs rather than using physical cables. Nonetheless, use of port channels is highly recommended, especially in a production deployment of ACE.

Figure 8-1illustrates a port channel interface.

Figure 8-1 Example of a Port Channel Interface



Related Topic

Configuring a Port-Channel Interface, page 8-3

Configuring a Port-Channel Interface

You can group physical ports together on the ACE to form a logical Layer 2 interface called the port-channel. All the ports belonging to the same port-channel must be configured with same values; for example, port parameters, VLAN membership, and 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.

Step 1 Select **Config > Virtual Contexts >** *context* **> Network > Port Channel Interfaces**. The Port Channel Interfaces table appears.

Step 2 Click **Add** to add a port channel interface, or select an existing port channel interface, then click **Edit** to modify it.

Note If you click **Edit**, not all of the fields can be modified.

Step 3 Enter the port channel interface attributes (see Table 8-1).

Table 8-1 Port Channel Interface Attributes

Field	Description
Interface Number	Specify a channel number for the port-channel interface, which can be from 1 to 255.
Description	Enter a brief description for this interface.
Fault Tolerance VLAN	Specify the fault tolerant (FT) VLAN used for communication between the members of the FT group
Admin Status	Indicate whether you want the interface to be Up or Down.
Load Balancing Method	Specify one of the following load balancing methods: • Dst-IP—Loads distribution on the destination IP address. • Dst-MAC—Loads distribution on the destination MAC address. • Dst-Port—Loads distribution on the destination TCP or UDP port. • Src-Dst-IP—Loads distribution on the source or destination IP address. • Src-Dst-MAC—Loads distribution on the source or destination MAC address. • Src-Dst-Port—Loads distribution on the source or destination port. • Src-IP—Loads distribution on the source IP address. • Src-MAC—Loads distribution on the source MAC address. • Src-Port—Loads distribution on the TCP or UDP source port.

Table 8-1 Port Channel Interface Attributes (continued)

Field	Description
Switch Port Type	Specify the interface switchport type: • N/A—Indicates that the switchport type is not specified. • Access—Specifies that the port interface is an access port. You must specify a VLAN as an access port in the Access VLAN field. • Trunk—Specifies that the port interface is a trunk port. When you select Trunk, you must complete the following fields: – Trunk Native VLAN—Identifies the 802.1Q native VLAN for a trunk. – Trunk Allowed VLANs—Selectively allocate individual VLANs to a trunk link.

Step 4 Click:

- **Deploy Now** to save your entries and to return to the Port Channel Interface table.
- **Cancel** to exit the procedure without saving your changes and to return to the Port Channel Interface table.
- **Next** to save your entries and to add another port-channel interface.

Configuring Gigabit Ethernet Interfaces

The ACE appliance provides physical Ethernet ports to connect servers, PCs, routers, and other devices to the ACE. The ACE supports four Layer 2 Ethernet ports for performing Layer 2 switching. 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, full-duplex, or half-duplex operation on an Ethernet LAN, and can carry traffic within a designated VLAN.

A Layer 2 Ethernet port can be configured as:

- **Member of Port-Channel Group—**The port is configured as a member of a port-channel group, which associates a physical port on the ACE to a logical port to create a port-channel logical interface. The VLAN association is derived from port-channel configuration. The port is configured as a Layer 2 EtherChannel, where each EtherChannel bundles the individual physical Ethernet data ports into a single logical link that provides the aggregate bandwidth of up to four physical links on the ACE.
- A**ccess VLAN—**The port is assigned to a single VLAN. This port is referred to as an access port and provides a connection for end users or node devices, such as a router or server.
- **Trunk port—**The port is associated with IEEE 802.1Q encapsulation-based VLAN trunking to allocate VLANs to ports and to pass VLAN information (including VLAN identification) between switches for all Ethernet channels defined in a Layer 2 Ethernet data port or a Layer 2 EtherChannel (port-channel) group on the ACE.

The following procedure describes how to configure a gigabit Ethernet interface.

Procedure

Step 1 Select **Config > Virtual Contexts >** *context* **> Network > Gigabit Ethernet Interfaces**. The GigabitEthernet Interfaces table appears.

Step 2 Select an existing gigabit Ethernet interface, then click **Edit** to modify it.

Step 3 Enter the Gigabit Ethernet physical interface attributes (see Table 8-2).

Table 8-2 Gigabit Ethernet Physical Interface Attributes

Field	Description
Interface Name	Name of the gigabit interface, which is the *slot_number*/*port_number* where *slot_number* is the physical slot on the ACE for the specified port, and *port_number* is the physical Ethernet data port on the ACE for the specified port.
Description	Enter a brief description for this interface.
Admin Status	Indicate whether you want the interface to be Up or Down.
Speed	Specifies the port speed, which can be • Auto—Autonegotiate with other devices • 10 Mbps • 100 Mbps • 1000 Mbps
Duplex	Specifies an interface duplex mode, which can be: • Auto—Resets the specified Ethernet port to automatically negotiate port speed and duplex of incoming signals. This is the default setting. • Half—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. • Full—Configures the specified Ethernet port for full-duplex operation, which allows data to travel in both directions at the same time.

Table 8-2 Gigabit Ethernet Physical Interface Attributes (continued)

Field	Description
Port Operation Mode	Specifies the port operation mode, which can be: • N/A—Indicates that this option is not to be used. • Channel Group—Specifies to map the port to a port channel. You must specify – Port Channel Group Number—Specify the port channel group number – Fault Tolerant VLAN—Specify the fault tolerant (FT) VLAN used for communication between the members of the FT group. • Switch Port—Specifies the interface switchport type: – Access —Specifies that the port interface is an access port. You must specify a VLAN as an access port in the Access VLAN field. – Trunk—Specifies that the port interface is a trunk port. When you select Trunk, you must complete one or both of the following fields: Trunk Native VLAN—Identifies the 802.1Q native VLAN for a trunk. Trunk Allowed VLANs—Selectively allocate individual VLANs to a trunk link.
Fault Tolerant VLAN	Specifies the fault tolerant (FT) VLAN used for communication between the members of the FT group.

Table 8-2 Gigabit Ethernet Physical Interface Attributes (continued)

Field	Description
Carrier Delay	Adds a configurable delay at the physical port level to address any issues with transition time, based on the variety of peers. Valid values are 0 to 120 seconds. The default is 0 (no carrier delay). **Note** 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. In this case, specify a carrier delay
QoS Trust COS	Enables Quality of Service (QoS) for the physical Ethernet port. By default, QoS is disabled for each physical Ethernet port on the ACE. QoS for a configured physical Ethernet port based on VLAN Classes of Service (CoS) bits (priority bits that segment the traffic in eight different classes of service). When you enable QoS on a port (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. In this case, heartbeat packets are always tagged with COS bits set to 7 (a weight of High). **Note** We recommend that you enable QoS on the FT VLAN port to provide higher priority for FT traffic.

Step 4 Click:

- **Deploy Now** to save your entries and to return to the Physical Interface table.
- **Cancel** to exit the procedure without saving your changes and to return to the Physical Interface table.
- **Next** or **Previous** to go to the next or previous physical channel.
- **Delete** to remove this entry from the Physical Interface table and to return to the table.

Related Topics

- Configuring Virtual Context VLAN Interfaces, page 8-8
- Configuring Virtual Context BVI Interfaces, page 8-19
- Configuring Virtual Context Static Routes, page 8-22

Configuring Virtual Context VLAN Interfaces

The ACE Appliance Device Manager uses class maps and policy maps to classify (filter) traffic and to direct it to different contexts. A virtual context uses VLANs to receive packets classified for that context.

Note When you create a new VLAN interface for a virtual context, you can configure one or more VLAN interfaces in any user context before you assign those VLAN interfaces to the associated user contexts in a virtual context through the Allocate-Interface VLANs field (see the "Creating Virtual Contexts" section on page 2-2).

Use this procedure to configure VLAN interfaces for virtual contexts.

Procedure

Step 1 To configure a virtual context, select **Config > Virtual Contexts >** *context* **> Network > VLAN Interfaces**. The VLAN Interface table appears.

Step 2 Click **Add** to add a new VLAN interface, or select an existing VLAN interface, then click **Edit** to modify it.

Note If you click **Edit**, not all of the fields can be modified.

Step 3 Enter the VLAN interface attributes (see Table 8-3). Click **More Settings** to access the additional VLAN interface attributes. By default, ACE appliance Device Manager hides the default VLAN interface attributes and the VLAN interface attributes which are not commonly used.

Note If you create a fault-tolerant VLAN, do not use it for any other network traffic.

Table 8-3 VLAN Interface Attributes

Field	Description
VLAN	Either accept the automatically incremented entry or enter a different value. Valid entries are integers from 2 to 4094.
Description	Enter a brief description for this interface.

Table 8-3 VLAN Interface Attributes (continued)

Field	Description
Interface Type	Select the role of the virtual context in the network topology of the VLAN interface: • Routed—In a routed topology, the ACE virtual context acts as a router between the client-side network and the server-side network. In this topology, every real server for the application must be routed through the ACE virtual context, either by setting the default gateway on each real server to the virtual contexts server-side VLAN interface address, or by using a separate router with appropriate routes configured between the ACE virtual context and the real servers. • Bridged—In a bridged topology, the ACE virtual context bridges two VLANs, a client-side VLAN and a real-server VLAN, on the same subnet using a bridged virtual interface (BVI). In this case, the real server routing does not change to accommodate the ACE virtual context. Instead, the ACE virtual context becomes a "bump in the wire" that transparently handles traffic to and from the real servers. • Unknown—Choose Unknown if you are unsure of the network topology of the VLAN interface.
IP Address	Enter the IP address assigned to this interface.
Alias IP Address	Enter the IP address of the alias this interface is associated with.
Peer IP Address	Enter the IP address of the remote peer.
Netmask	Select the subnet mask to be used.
Admin Status	Indicate whether you want the interface to be Up or Down.
Enable MAC Sticky	Check the check box to indicate that the ACE appliance is to convert dynamic MAC addresses to sticky secure MAC addresses and add this information to the running configuration. Clear the check box to indicate that the ACE appliance is not to convert dynamic MAC addresses to sticky secure MAC addresses.
Enable Normalization	Check the check box to indicate that normalization is to be enabled on this interface. Clear the check box to indicate that normalization is to be disabled on this interface. **Caution** Disabling normalization may expose your ACE appliance and network to potential security risks. Normalization protects your networking environment from attackers by enforcing strict security policies that are designed to examine traffic for malformed or malicious segments.

Table 8-3 VLAN Interface Attributes (continued)

Field	Description
More Settings	
Secondary IP Groups	This option appears only when Interface Type is set to Routed. Enter a maximum of four secondary IP groups for the VLAN. The IP, alias IP, and peer IP addresses of each Secondary IP Group should be in the same subnet. **Note** You cannot configure secondary IP addresses on FT VLANs. To create up to four secondary IP groups for the VLAN, do the following: **a.** Define one or more of the following secondary IP address types: – IP—Secondary IP address assigned to this interface.The primary address must be active for the secondary address to be active. – AliasIP—Secondary IP address of the alias associated with this interface. – PeerIP—Secondary IP address of the remote peer. – Netmask—Secondary subnet mask to be used. The ACE has a system limit of 1,024 for each secondary IP address type. **b.** Click **Add to selection** (right arrow) to add the group to the group display area. **c.** Repeat Steps 1 and 2 for each additional group. **d.** (Optional) Rearrange the order in which the groups are listed by selecting one of the group listings in the group display area and click either **Move item up in list** (up arrow) or **Move item down in list** (down arrow). Note that the ACE does not care what order the groups are in. **e.** (Optional) Edit a group or remove it from the list by selecting the desired group in the group display area and click **Remove from selection** (left arrow).

Table 8-3 VLAN Interface Attributes (continued)

Field	Description
ARP Inspection Type	By default, ARP inspection is disabled on all interfaces, allowing all ARP packets through the ACE. When you enable ARP inspection, the ACE appliance uses the IP address and interface ID (ifID) of an incoming ARP packet as an index into the ARP table. ARP inspection operates only on ingress bridged interfaces. ARP inspection prevents malicious users from impersonating other hosts or routers, known as ARP spoofing. ARP spoofing can enable a "man-in-the-middle" attack. For example, a host sends an ARP request to the gateway router. The gateway router responds with the gateway router MAC address. **Note** If ARP inspection fails, then the ACE does not perform source MAC validation. The options are as follows: • N/A—ARP inspection is disabled. • Flood—Enables ARP forwarding of nonmatching ARP packets. The ACE appliance forwards all ARP packets to all interfaces in the bridge group. This is the default setting. In the absence of a static ARP entry, this option bridges all packets. • No-flood—Disables ARP forwarding for the interface and drops nonmatching ARP packets. In the absence of a static ARP entry, this option does not bridge any packets.
Max. Fragment Chains Allowed	Enter the maximum number of fragments belonging to the same packet that the ACE appliance is to accept for reassembly. Valid entries are integers from 1 to 256.
Min. Fragment MTU Value	Enter the minimum fragment size that the ACE appliance accepts for reassembly for a VLAN interface. Valid entries are integers from 28 to 9216 bytes.
MTU Value	Enter number of bytes for Maximum Transmission Units (MTUs). Valid entries are integers from 68 to 9216, and the default is 1500.
Reassembly Timeout (Seconds)	Enter the number of seconds that the ACE appliance is to wait before it abandons the fragment reassembly process if it doesn't receive any outstanding fragments for the current fragment chain (that is, fragments belonging to the same packet). Valid entries are 1 to 30 seconds.
Reverse Path Forwarding (RPF)	Check the check box to indicate that the ACE appliance is to discard IP packets if no reverse route is found or if the route does not match the interface on which the packets arrived. Clear the check box to indicate that the ACE appliance is not to filter or discard packets based on the ability to verify the source IP address.
Enable MAC Address Autogenerate	Allows you to configure a different MAC address for the VLAN interface.

Table 8-3 VLAN Interface Attributes (continued)

Field	Description
Enable ICMP Guard	Check the check box to indicate that ICMP Guard is to be enabled on the ACE appliance. Clear the check box to indicate that ICMP Guard is not to be enabled on ACE appliance. **Caution** Disabling ICMP security checks may expose your ACE appliance and network to potential security risks. When you disable ICMP Guard, the ACE appliance no longer performs NAT translations on the ICMP header and payload in error packets, which can potentially reveal real host IP addresses to attackers.
Enable DHCP Relay	Check the check box to indicate that the ACE appliance is to accept DHCP requests from clients on this interface and to enable the DHCP relay agent. Clear the check box to indicate that the ACE appliance is not to accept DHCP requests or enable the DHCP relay agent.
Action For DF Bit	Indicate how the ACE appliance is to handle a packet that has it DF (Don't Fragment) bit set in the IP header: • Allow—Indicates that the ACE appliance is to permit the packet with the DF bit set. If the packet is larger than the next-hop MTU, ACE appliance discards the packet and sends an ICMP unreachable message to the source host. • Clear—Indicates that the ACE appliance is to clear the DF bit and permit the packet. If the packet is larger than the next-hop MTU, the ACE appliance fragments the packet. The default is Allow.
Action For IP Header Options	Select the action the ACE appliance is to take when an IP option is set in a packet: • Allow—Indicates that the ACE appliance is to allow the IP packet with the IP options set. • Clear—Indicates that the ACE appliance is to clear all IP options from the packet and to allow the packet. • Clear-Invalid—Indicates that the ACE appliance is to clear the invalid IP options from the packet and then allow the packet. • Drop—Indicates that the ACE appliance is to discard the packet regardless of any options that are set.
Min. TTL IP Header Value	Enter the minimum number of hops a packet is allowed to reach its destination. Valid entries are integers from 1 to 255. Each router along the packet's path decrements the TTL by one. If the packet's TTL reaches zero before the packet reaches its destination, the packet is discarded.
Enable Syn Cookie Threshold Value	Embryonic connection threshold above which the ACE applies SYN-cookie DoS protection. Valid entries are integers from 1 to 65535.

Table 8-3 VLAN Interface Attributes (continued)

Field	Description
UDP Config Commands	Select the UDP boost command: • N/A—not applicable • IP Destination Hash—Performs destination IP hash during connection. • IP Source Hash—Performs source IP hash during connection lookup.
Input Policies	From the Available list, double-click the policy map name that is associated with this VLAN interface or use the right arrow to move it to the Selected list. This policy map is to be applied to the inbound direction of the interface; that is, all traffic received by this interface. If you choose more than one policy map, use the Up and Down arrows to choose the priority of the policy map in the Selected list. These arrows modify the order of the policy maps for new VLANs only; they do not modify the policy map order when editing an existing policy map.
Input Access Group	From the Available list, double-click an ACL name for the ACL input access group to be associated with this VLAN interface or use the right arrow to move it to the Selected list. Any ACL group listed in the Selected list specifies that this access group is to be applied to the inbound direction of the interface.
Output Access Group	From the Available list, double-click an ACL name for the ACL output access group that is associated with this VLAN interface or use the right arrow to move it to the Selected list. Any ACL group listed in the Selected list specifies that this access group is to be applied to the outbound direction of the interface; that is, all traffic sent by this interface.
Static ARP Entry (IP/MAC Address)	For the Static ARP entry, do the following: **a.** In the ARP IP Address field, enter the IP address in dotted-decimal notation (for example, 192.168.11.2). **b.** In the ARP MAC Address field, enter the hardware MAC address for the ARP table entry (for example, 00.02.9a.3b.94.d9). **c.** When completed, use the right arrow to move the static ARP entry to the list box. Use the Up and Down arrows to choose the priority of the static ARP entry in the list box. These arrows modify the order of the static ARPs for new VLANs only; they do not modify the static ARP order when editing an existing policy map.
DHCP Relay Configuration	Enter the IP address of the DHCP server to which the DHCP relay agent is to forward client requests. Enter the IP address in dotted-decimal notation, such as 192.168.11.2.

Step 4 Click:

- **Deploy Now** to save your entries and to return to the VLAN Interface table.
- **Cancel** to exit the procedure without saving your changes and to return to the VLAN Interface table.
- **Next** to save your entries and to add another VLAN interface.

Related Topics

- Configuring VLAN Interface Options, page 8-14

Viewing All VLAN Interfaces

Use this procedure to view all VLAN interfaces.

Procedure

Step 1 Select **Config > Virtual Contexts >** *context* **> Network > VLAN Interfaces**.

The VLAN Interface table appears listing all VLAN interfaces for the selected virtual context.

Related Topics

- Configuring Virtual Context VLAN Interfaces, page 8-8
- Configuring VLAN Interface Options, page 8-14
- Configuring VLAN Interface Policy Map Use, page 8-15

Configuring VLAN Interface Options

After adding a VLAN interface, you can configure other VLAN interface attributes such as policy map use, access groups, static ARP entries, and so on. The tabs for these attributes appear beneath the VLAN Interface table or below the VLAN Interface configuration screen after you have added a new VLAN interface.

Configuration options for VLAN interfaces are:

- Configuring VLAN Interface Policy Map Use, page 8-15
- Configuring VLAN Interface Access Control, page 8-16
- Configuring VLAN Interface Static ARP Entries, page 8-17
- Configuring VLAN Interface NAT Pools, page 8-17
- Configuring VLAN Interface DHCP Relay, page 8-19

Configuring VLAN Interface Policy Map Use

Use this procedure to associate a policy map with a VLAN interface.

Assumptions

- You have successfully configured at least one VLAN interface (see Configuring Virtual Context VLAN Interfaces, page 8-8).
- A Layer 3/Layer 4 or Management policy map has been configured for this virtual context. For more information, see Configuring Traffic Policies, page 10-1.

Procedure

Step 1 Select **Config > Virtual Contexts >** *context* **> Network > VLAN Interfaces**.

The VLAN Interfaces table appears.

Step 2 Select the VLAN interface you want to associate with a policy map, then select the Policy tab. The Policy table appears.

Step 3 Click **Add** to add a policy. The Policy configuration screen appears.

Step 4 In the Policy Map field, select the policy map to be associated with this VLAN interface.

Note The Device Manager considers an interface as a management interface if it has a management policy map associated with the VLAN interface. See the "Creating Virtual Contexts" section on page 2-2.

Step 5 In the Direction field, input is automatically specified; this policy map is to be applied to the inbound direction of the interface; that is, all traffic received by this interface.

Step 6 Click:

- **Deploy Now** to save your entries and to return to the Policy table.
- **Cancel** to exit this procedure without saving your entries and to return to the Policy table.
- **Next** to save your entries and to add another policy to this interface.

Related Topics

- Configuring VLAN Interface Access Control, page 8-16
- Configuring VLAN Interface Static ARP Entries, page 8-17
- Configuring VLAN Interface NAT Pools, page 8-17
- Configuring VLAN Interface DHCP Relay, page 8-19

Configuring VLAN Interface Access Control

The ACE Appliance Device Manager uses access control lists to limit access to and from VLAN interfaces in a virtual context. Use this procedure to configure access control for a VLAN interface.

Assumptions

- You have successfully configured at least one VLAN interface (see Configuring Virtual Context VLAN Interfaces, page 8-8).
- An access control list has been configured for this virtual context. Entering an ACL name does not configure the ACL; you must configure the ACL on the ACE appliance. For more information, see Configuring Virtual Context Expert Options, page 2-69.

Procedure

Step 1 Select **Config > Virtual Contexts >** *context* **> Network > VLAN Interfaces**.

The VLAN Interfaces table appears.

Step 2 Select the VLAN interface you want to associate with an ACL, then select the Access Group tab. The Access Group table appears.

Step 3 Click **Add** to associate a new ACL with the selected VLAN interface. The Access Group configuration screen appears.

Step 4 In the ACL Name field, select the ACL group to be associated with this VLAN interface.

Step 5 In the Direction field, select the traffic this access group applies to:

- Input—Specifies that this access group is to be applied to the inbound direction of the interface; that is, all traffic received by this interface.
- Output—Specifies that this access group is to be applied to the outbound direction of the interface; that is, all traffic sent by this interface.

Step 6 Click:

- **Deploy Now** to save your entries and to return to the Access Group table.
- **Cancel** to exit this procedure without saving your entries and to return to the Access Group table.
- **Next** to save your entries and to apply another access group to this interface.

Related Topics

- Configuring VLAN Interface Policy Map Use, page 8-15
- Configuring VLAN Interface Static ARP Entries, page 8-17
- Configuring VLAN Interface NAT Pools, page 8-17
- Configuring VLAN Interface DHCP Relay, page 8-19

Configuring VLAN Interface Static ARP Entries

Use this procedure to configure static ARP entries for a VLAN interface.

Assumption

You have successfully configured at least one VLAN interface (see Configuring Virtual Context VLAN Interfaces, page 8-8).

Procedure

Step 1 Select **Config > Virtual Contexts >** *context* **> Network > VLAN Interfaces**.

The VLAN Interface table appears.

Step 2 Select the VLAN interface you want to configure static ARP entries for, then select the Static ARP Entries tab. The Static ARP Entries table appears.

Step 3 Click **Add** to add a new entry. The Static ARP Entries configuration screen appears.

Step 4 In the ARP IP Address field, enter the IP address in dotted-decimal notation (for example, 192.168.11.2).

Step 5 In the ARP MAC Address field, enter the hardware MAC address for the ARP table entry (for example, 00.02.9a.3b.94.d9).

Step 6 Click:

- **Deploy Now** to save your entries and to return to the Static ARP Entries table.
- **Cancel** to exit this procedure without saving your entries and to return to the Static ARP Entries table.
- **Next** to save your entries and to add another static ARP entry.

Related Topics

- Configuring VLAN Interface Policy Map Use, page 8-15
- Configuring VLAN Interface Access Control, page 8-16
- Configuring VLAN Interface NAT Pools, page 8-17
- Configuring VLAN Interface DHCP Relay, page 8-19

Configuring VLAN Interface NAT Pools

Network Address Translation (NAT) is designed to simplify and conserve IP addresses. It allows private IP networks that use unregistered IP addresses to connect to the Internet. NAT operates on a router, usually connecting two networks, and translates the private (not globally unique) addresses in the internal network into legal addresses before the packets are forwarded to another network.

The ACE Appliance Device Manager allows you to configure NAT so that it advertises only one address for the entire network to the outside world. This effectively hides the entire internal network behind that address, thereby offering both security and address conservation.

Several internal addresses can be translated to only one or a few external addresses by using Port Address Translation (PAT) in conjunction with NAT. With PAT, you can configure static address translations at the port level and use the remainder of the IP address for other translations. PAT effectively extends NAT from one-to-one to many-to-one by associating the source port with each flow.

Use this procedure to configure NAT pools for a VLAN interface.

Assumption

You have successfully configured at least one VLAN interface (see Configuring Virtual Context VLAN Interfaces, page 8-8).

Procedure

Step 1 Select **Config > Virtual Contexts >** *context* **> Network > NAT**.

The NAT Pool table appears.

Step 2 In the NAT Pool table, click **Add** to add a new entry. The NAT Pool configuration screen appears.

Step 3 Select the VLAN interface you want to configure a NAT pool.

Step 4 In the NAT Pool Id field, either accept the automatically incremented entry or enter a new number to uniquely identify this pool. Valid entries are integers from 1 to 2147483647.

Step 5 In the Start IP Address field, enter an IP address in dotted-decimal notation (such as 192.168.11.2). This entry identifies either a single IP address or, if using a range of IP addresses, the first IP address in a range of global addresses for this NAT pool.

Step 6 In the End IP Address field, enter the highest IP address in a range of global IP addresses for this NAT pool. Enter the IP address in dotted-decimal notation, such as 192.168.11.2.

Leave this field blank if you want to identify only the single IP address in the Start IP Address field.

Step 7 In the Netmask field, select the subnet mask for the global IP addresses in the NAT pool.

Step 8 Check the PAT Enabled check box to indicate that the ACE appliance is to perform port address translation (PAT) in addition to NAT. Clear the check box to indicate that the ACE appliance is not to perform port address translation (PAT) in addition to NAT.

Step 9 Click:

- **Deploy Now** to save your entries and to return to the NAT Pool table.
- **Cancel** to exit this procedure without saving your entries and to return to the NAT Pool table.
- **Next** to save your entries and to add another NAT Pool entry.

Related Topics

- Configuring VLAN Interface Policy Map Use, page 8-15
- Configuring VLAN Interface Access Control, page 8-16
- Configuring VLAN Interface Static ARP Entries, page 8-17
- Configuring VLAN Interface DHCP Relay, page 8-19

Configuring VLAN Interface DHCP Relay

Use this procedure to configure DHCP relay for a VLAN interface.

Assumption

You have successfully configured at least one VLAN interface (see Configuring Virtual Context VLAN Interfaces, page 8-8).

Procedure

Step 1 Select **Config > Virtual Contexts >** *context* **> Network > VLAN Interfaces**.

The VLAN Interfaces table appears.

Step 2 Select the VLAN interface you want to configure DHCP relay for, then select the DHCP Relay Configuration tab. The DHCP Relay Configuration table appears.

Step 3 Click **Add** to add a new entry. The DHCP Relay Configuration screen appears.

Step 4 In the IP Address field, enter the IP address of the DHCP server to which the DHCP relay agent is to forward client requests. Enter the IP address in dotted-decimal notation, such as 192.168.11.2.

Step 5 Click:

- **Deploy Now** to save your entries and to return to the DHCP Relay Configuration table.
- **Cancel** to exit this procedure without saving your entries and to return to the DHCP Relay Configuration table.
- **Next** to save your entries and to add another DHCP relay entry.

Related Topics

- Configuring VLAN Interface Policy Map Use, page 8-15
- Configuring VLAN Interface Access Control, page 8-16
- Configuring VLAN Interface NAT Pools, page 8-17
- Configuring VLAN Interface Static ARP Entries, page 8-17

Configuring Virtual Context BVI Interfaces

The ACE Appliance Device Manager supports virtual contexts containing Bridge-Group Virtual Interfaces (BVI). Use this procedure to configure BVI interfaces for virtual contexts.

Procedure

Step 1 Select **Config > Virtual Contexts >** *context* **> Network > BVI Interfaces**.

The BVI Interface tables appears.

Step 2 Click **Add** to add a new BVI interface, or select an existing BVI interface, then click **Edit** to modify it.

Note If you click **Edit**, not all of the fields can be modified.

Step 3 Enter the interface attributes (see Table 8-4).

Table 8-4 BVI Interface Attributes

Field	Description
BVI	Either accept the automatically incremented entry or enter a different, unique value. Valid entries are integers from 1 to 4094.
Description	Enter a brief description for this interface.
IP Address	Enter the IP address assigned to this interface.
Alias IP Address	Enter the IP address of the alias this interface is associated with.
Peer IP Address	Enter the IP address of the remote peer.
Netmask	Select the subnet mask to be used.
Enable MAC Address Autogenerate	Allows you to configure a different MAC address for the BVI interface.
Admin Status	Indicate whether you want the interface to be Up or Down.
Secondary IP Groups	(Optional) Enter a maximum of four secondary IP groups for the BVI. To create up to four secondary IP groups for this BVI, do the following: **a.** Define one or more of the following secondary IP address types: – IP—Secondary IP address assigned to this interface.The primary address must be active for the secondary address to be active. – AliasIP—Secondary IP address of the alias associated with this interface. – PeerIP—Secondary IP address of the remote peer. – Netmask—Secondary subnet mask to be used. The ACE has a system limit of 1,024 for each secondary IP address type. **b.** Click Add to selection (right arrow) to add the group to the group display area. **c.** Repeat Steps 1 and 2 for each additional group. **d.** (Optional) Rearrange the order in which the groups are listed by selecting one of the group listings in the group display area and click either Move item up in list (up arrow) or Move item down in list (down arrow). Note that the ACE does not care what order the groups are in. **e.** (Optional) Edit a group or remove it from the list by selecting the desired group in the group display area and click Remove from selection (left arrow).
First VLAN	Enter the first VLAN whose bridge group is to be configured with this BVI. This VLAN can be the server or client VLAN. Valid entries are from 2 to 4094.
First VLAN Description	Enter a brief description for the first VLAN.

Table 8-4 BVI Interface Attributes (continued)

Field	Description
Second VLAN	Enter the second VLAN whose bridge group is to be configured with this BVI. This VLAN can be the server or client VLAN. Valid entries are from 2 to 4094.
Second VLAN Description	Enter a brief description for the second VLAN.

Step 4 Click:

- **Deploy Now** to save your entries and to return to the BVI Interface table.
- **Cancel** to exit the procedure without saving your entries and to return to the BVI Interface table.
- **Next** to save your entries and to configure another BVI interface for this context.

Related Topics

- Configuring Network Access, page 8-1
- Configuring Virtual Context Primary Attributes, page 2-11
- Configuring Virtual Context VLAN Interfaces, page 8-8
- Configuring Virtual Context Syslog Logging, page 2-12
- Configuring Traffic Policies, page 10-1

Viewing All BVI Interfaces by Context

To view all BVI interfaces associated with a specific virtual context, select **Config > Virtual Contexts >** *context* **> Network > BVI Interfaces**.

The BVI Interface table appears with the information shown in Table 8-5.

Table 8-5 BVI Interface Fields

Field	Description
Bridge Group Number	Name of the interface.
Description	Description for this interface.
IP Address	IP address assigned to this interface.
Netmask	Subnet mask for this interface.
Admin Status	The status of the interface, which can be Up or Down.
First VLAN	First VLAN whose bridge group is to be configured with this BVI. This VLAN can be the server or client VLAN.
First VLAN Description	Description for the first VLAN.
Second VLAN	Second VLAN whose bridge group is to be configured with this BVI. This VLAN can be the server or client VLAN.
Second VLAN Description	Description for the second VLAN.

Related Topics

- Configuring Virtual Context VLAN Interfaces, page 8-8
- Using Virtual Contexts, page 2-2
- Configuring Virtual Context Primary Attributes, page 2-11
- Configuring Virtual Context VLAN Interfaces, page 8-8
- Configuring Virtual Context Syslog Logging, page 2-12
- Configuring Traffic Policies, page 10-1

Configuring Virtual Context Static Routes

Note This functionality is available for only Admin virtual contexts.

Admin and user context modes do not support dynamic routing, therefore you must use static routes for any networks to which the ACE appliance is not directly connected, such as when there is a router between a network and the ACE appliance.

Procedure

Step 1 Select **Config > Virtual Contexts >** *context* **> Network > Static Routes**.

The Static Route table appears.

Step 2 To add a static route for this context, click **Add**.

Note You cannot modify an existing static route. To make changes to an existing static route, you must delete the static route and then add it back.

Step 3 In the Destination Prefix field, enter the IP address for the route. The address you specify for the static route is the address that is in the packet before entering the ACE appliance and performing network address translation. Enter the address in dotted-decimal IP notation (for example, 192.168.11.2).

Step 4 In the Destination Prefix Mask field, select the subnet to use for this route.

Step 5 In the Next Hop field, enter the IP address of the gateway router for this route. The gateway address must be in the same network as a VLAN interface for this context.

Step 6 Click:

- **Deploy Now** to save your entries and to return to the Static Route table.
- **Cancel** to exit this procedure without saving your entries and to return to the Static Route table.
- **Next** to save your entries and to add another static route.

Related Topics

- Configuring Virtual Contexts, page 2-7
- Configuring Virtual Context Primary Attributes, page 2-11

- Managing ACE Appliance Licenses, page 2-27
- Configuring High Availability, page 9-1

Viewing All Static Routes by Context

Use this procedure to view all static routes associated with a virtual context.

Procedure

Step 1 Select **Config > Virtual Contexts >** *context* **> Network > Static Routes**.

The Static Route table appears with the following information:

- Destination prefix
- Destination prefix mask
- Next hop IP address

Related Topics

- Configuring Virtual Context Static Routes, page 8-22
- Configuring Virtual Context VLAN Interfaces, page 8-8

Configuring Global IP DHCP

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

The following steps show you how to configure the DHCP relay agent at the context level so the configuration applies to all interfaces associated with the context.

Note The options that appear when you select **Config > Virtual Contexts >** ***context*** depend on the device associated with the virtual context and the role associated with your account.

Procedure

Step 1 Select **Config > Virtual Contexts >** *context* **> Network > Global IP DHCP**. The Global IP DHCP configuration table appears.

Step 2 Click **Enable DHCP Relay For The Context** to enable DHCP relay for the context and all interfaces associated with this context.

Step 3 Select a relay agent information forwarding policy, which can be

- N/A—Specifies to not configure the DHCP relay to identify what is to be performed if a forwarded message already contains relay information.
- Keep—Specifies that existing information is left unchanged on the DHCP relay agent.
- Replace—Specifies that existing information is overwritten on the DHCP relay agent.

Step 4 In the IP DHCP Server field, select the IP DHCP server to which the DHCP relay agent is to forward client requests.

Step 5 Click:

- **Deploy Now** to immediately deploy this configuration. This option appears for virtual contexts.
- **Cancel** to exit this procedure without saving your entries and to return to the previous table.
- **Next** to deploy your entries and to add another DHCP relay entry.