



CHAPTER 9

Configuring Network Access

Revised Date: 2/18/09

The ANM uses class maps and policy maps to classify (filter) traffic and to direct it to different ACE appliances.

The following sections explain how to configure network access using ANM:

- [Configuring VLAN Interfaces, page 9-2](#)
- [Configuring Virtual Context BVI Interfaces, page 9-12](#)
- [Configuring Virtual Context Static Routes, page 9-14](#)
- [Configuring Global IP DHCP, page 9-16](#)
- [Configuring Static VLANs for Over 8 K Static NAT Configurations, page 9-16](#)
- [Configuring Gigabit Ethernet Interfaces, page 9-17](#)
- [Configuring Port Channel Interfaces, page 9-21](#)

VLAN Overview

The following sections describe VLANs:

- [ACE Module VLAN Overview, page 9-1](#)
- [ACE Appliance VLAN Overview, page 9-2](#)

ACE Module VLAN Overview

The ACE module does not include any external physical interfaces to receive traffic from clients and servers. Instead, it uses internal VLAN interfaces. You assign VLANs from the supervisor to the ACE. After the VLANs are assigned to the ACE, you can configure the corresponding VLAN interfaces on the ACE as either routed or bridged for use. When you configure an IP address on an interface, the ACE automatically makes it a routed mode interface.

Similarly, when you configure a bridge group on an interface VLAN, the ACE automatically makes it a bridged interface. Then, you associate a bridge-group virtual interface (BVI) with the bridge group. For more information on bridged groups and BVIs, see [Configuring Virtual Context BVI Interfaces, page 9-12](#).

The ACE 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.

Related Topics

- [Configuring VLAN Interfaces, page 9-2](#)
- [Configuring VLAN Interface Options, page 9-7](#)
- [Configuring Virtual Context BVI Interfaces, page 9-12](#)
- [Configuring Virtual Context Static Routes, page 9-14](#)
- [Configuring Global IP DHCP, page 9-16](#)

ACE Appliance VLAN Overview

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.

Related Topics

- [Configuring VLAN Interfaces, page 9-2](#)
- [Configuring VLAN Interface Options, page 9-7](#)
- [Configuring Virtual Context BVI Interfaces, page 9-12](#)
- [Configuring Gigabit Ethernet Interfaces, page 9-17](#)
- [Configuring Port Channel Interfaces, page 9-21](#)

Configuring VLAN Interfaces

Use this procedure to configure VLAN interfaces for virtual contexts on the ACE.



Note

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

Procedure

Step 1 Select the item to configure:

- To configure a virtual context, select **Config > Devices > context > Network > VLAN Interfaces**.
- To configure a configuration building block, select **Config > Global > All Building Blocks > building_block > 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 9-1](#)).

Enable MAC address autogenerate.



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

Table 9-1 *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.
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.
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, and the default is 112.

Table 9-1 VLAN Interface Attributes (continued)


Field	Description
ARP Inspection Type	<p>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.</p> <p>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.</p> <p> Note If ARP inspection fails, then the ACE does not perform source MAC validation.</p> <p>The options are as follows:</p> <ul style="list-style-type: none"> • 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.
Fragment Min MTU Value	Enter the minimum Maximum Transmission Units (MTUs) for each allowable fragment. Valid entries are integers from 28-9216 with no default.
Min MTU Value	Enter number of bytes for MTU). Valid entries are integers from 68 to 9216, and the default is 1500.
Reassembly Timeout	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)	<p>Select the checkbox 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.</p> <p>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.</p>
Bridge Group Number	Enter the number of the bridge group to be configured on this VLAN. When you configure a bridge group on a VLAN, the ACE appliance automatically makes it bridged. Valid entries are from 1 to 4094.

Table 9-1 VLAN Interface Attributes (continued)



Field	Description
Enable MAC Sticky	<p>Select 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.</p> <p>Clear the check box to indicate that the ACE appliance is not to convert dynamic MAC addresses to sticky secure MAC addresses.</p>
Enable ICMP Guard	<p>Select the check box to indicate that ICMP Guard is to be enabled on the ACE appliance.</p> <p>Clear the check box to indicate that ICMP Guard is not to be enabled on ACE appliance.</p> <p> 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.</p>
Enable DHCP Relay	<p>Select 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.</p> <p>Clear the check box to indicate that the ACE appliance is not to accept DHCP requests or enable the DHCP relay agent.</p>
Enable Normalization	<p>Select the check box to indicate that normalization is to be enabled on this interface.</p> <p>Clear the check box to indicate that normalization is to be disabled on this interface.</p> <p> 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.</p>
Action for DF Bit	<p>Indicate how the ACE appliance is to handle a packet that has its DF (Don't Fragment) bit set in the IP header:</p> <ul style="list-style-type: none"> • 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.

Table 9-1 VLAN Interface Attributes (continued)

Field	Description
Action for IP Header Options	Select the action the ACE appliance is to take when an IP option is set in a packet: <ul style="list-style-type: none"> • 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	For ACE 2.0 and 3.0 devices only. Embryonic connection threshold above which the ACE applies SYN-cookie DoS protection. Valid entries are integers from 2 to 65535.
UDP Config Commands	For ACE 2.0 and 3.0 devices only. Select the UDP boost command: <ul style="list-style-type: none"> • N/A—not applicable • IP-Destination-Hash—Perform source IP hash during connection lookup • IP-Source-Hash—Perform destination IP hash during connection
Enable MAC Address Autogenerate	Allows you to configure a different MAC address for the VLAN interface.

Step 4 Click:

- **Deploy Now** to immediately deploy this configuration. This option appears for virtual contexts.
- **OK** to save your entry. This option appears for configuration building blocks.
- **Cancel** to exit this procedure without saving your entries and to return to the previous screen.
- **Next** to deploy your entries and to create another VLAN interface.

Related Topic

[Configuring VLAN Interface Options, page 9-7](#)

Viewing All VLAN Interfaces

Use this procedure to view all VLAN interfaces.

Procedure

Step 1 Select **Config > Devices > context > Network > VLAN Interfaces**.

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

Related Topics

- [Configuring VLAN Interfaces, page 9-2](#)
- [Configuring VLAN Interface Options, page 9-7](#)
- [Configuring VLAN Interface Policy Map Use, page 9-7](#)

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.

You might need to click the toggle button to switch from Browse mode to Configuration mode to enter the interface options.

Configuration options for VLAN interfaces are:

- [Configuring VLAN Interface Policy Map Use, page 9-7](#)
- [Configuring VLAN Interface Access Control, page 9-8](#)
- [Configuring VLAN Interface Static ARP Entries, page 9-9](#)
- [Configuring VLAN Interface NAT Pools, page 9-10](#)
- [Configuring VLAN Interface DHCP Relay, page 9-12](#)

Configuring VLAN Interface Policy Map Use

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



Note

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

Assumptions

- You have successfully configured at least one VLAN interface (see [Configuring VLAN Interfaces, page 9-2](#)).
- A Layer 3/Layer 4 or Management policy map has been configured for this virtual context. For more information, see [Configuring Traffic Policies, page 11-1](#).

Procedure

Step 1 Select the item to configure:

- To configure a virtual context, select **Config > Devices > context > Network > VLAN Interfaces**.

- To configure a configuration building block, select **Config > Global > All Building Blocks > building_block > Network > VLAN Interfaces**.
- Step 2** Select the VLAN interface you want to associate with a policy map, then select the Policy tab. The Policy configuration 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.
- Step 5** In the Direction field, select the traffic this policy map applies to:
- **Input**—Specifies that this policy map is to be applied to the inbound direction of the interface; that is, all traffic received by this interface.
 - **Output**—Specifies that this policy map 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 immediately deploy this configuration. This option appears for virtual contexts.
 - **OK** to save your entry. This option appears for configuration building blocks.
 - **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 policy to this interface.
-

Related Topics

- [Configuring VLAN Interface Options, page 9-7](#)
- [Configuring VLAN Interface Access Control, page 9-8](#)
- [Configuring VLAN Interface Static ARP Entries, page 9-9](#)
- [Configuring VLAN Interface NAT Pools, page 9-10](#)
- [Configuring VLAN Interface DHCP Relay, page 9-12](#)

Configuring VLAN Interface Access Control

The ACE 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.



Note

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

Assumptions

- You have successfully configured at least one VLAN interface (see [Configuring VLAN Interfaces, page 9-2](#)).
- 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 Security with ACLs, page 3-43](#).

Procedure

-
- Step 1** Select the item to configure:
- To configure a virtual context, select **Config > Devices > context > Network > VLAN Interfaces**.
 - To configure a configuration building block, select **Config > Global > All Building Blocks > building_block > Network > VLAN Interfaces**.
- The VLAN Interface table appears.
- Step 2** Select the VLAN interface you want to associate with an ACL, then select the Access Group tab. The Access Group configuration 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 immediately deploy this configuration. This option appears for virtual contexts.
 - **OK** to save your entry. This option appears for configuration building blocks.
 - **Cancel** to exit this procedure without saving your entries and to return to the previous screen.
 - **Next** to deploy your entries and to apply another access group to this interface.
-

Related Topics

- [Configuring VLAN Interface Policy Map Use, page 9-7](#)
- [Configuring VLAN Interface Static ARP Entries, page 9-9](#)
- [Configuring VLAN Interface NAT Pools, page 9-10](#)
- [Configuring VLAN Interface DHCP Relay, page 9-12](#)

Configuring VLAN Interface Static ARP Entries

Use this procedure to configure static ARP entries for a VLAN interface on the ACE appliance.



Note

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

Assumption

You have successfully configured at least one VLAN interface (see [Configuring VLAN Interfaces, page 9-2](#)).

Procedure

-
- Step 1** Select the item to configure:
- To configure a virtual context, select **Config > Devices > context > Network > VLAN Interfaces**.
 - To configure a configuration building block, select **Config > Global > All Building Blocks > building_block > Network > VLAN Interfaces**.
- The VLAN Interface table appears.
- Step 2** Select the VLAN interface for which you want to configure static ARP entries, then click the Static ARP Entries tab. The Static ARP Entries configuration table appears.
- Step 3** In the Static ARP table, click **Add** to configure static ARP entries for the selected VLAN interface.
- 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 immediately deploy this configuration. This option appears for virtual contexts.
 - OK** to save your entry. This option appears for configuration building blocks.
 - Cancel** to exit this procedure without saving your entries and to return to the previous screen.
 - Next** to deploy your entries and to add another static ARP entry.
-

Related Topics

- [Configuring VLAN Interface Policy Map Use, page 9-7](#)
- [Configuring VLAN Interface Access Control, page 9-8](#)
- [Configuring VLAN Interface NAT Pools, page 9-10](#)
- [Configuring VLAN Interface DHCP Relay, page 9-12](#)

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 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.

**Note**

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

Assumption

You have successfully configured at least one VLAN interface (see [Configuring VLAN Interfaces, page 9-2](#)).

Procedure

-
- Step 1** Select the item to configure:
- To configure a virtual context, select **Config > Devices > context > Network > VLAN Interfaces**.
 - To configure a configuration building block, select **Config > Global > All Building Blocks > building_block > Network > VLAN Interfaces**.
- Step 2** Select the VLAN interface you want to configure a NAT pool for, then select NAT Pool tab. The NAT Pool configuration table appears.
- Step 3** Click **Add** to add a new entry.
- Step 4** In the NAT 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** Select 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 immediately deploy this configuration. This option appears for virtual contexts.
 - **OK** to save your entry. This option appears for configuration building blocks.
 - **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 NAT Pool entry.
-

Related Topics

- [Configuring VLAN Interface Policy Map Use, page 9-7](#)
- [Configuring VLAN Interface Access Control, page 9-8](#)
- [Configuring VLAN Interface Static ARP Entries, page 9-9](#)
- [Configuring VLAN Interface DHCP Relay, page 9-12](#)

Configuring VLAN Interface DHCP Relay

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



Note

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

Assumption

You have successfully configured at least one VLAN interface (see [Configuring VLAN Interfaces, page 9-2](#)).

Procedure

-
- Step 1** Select the item to configure:
- To configure a virtual context, select **Config > Devices > context > Network > VLAN Interfaces**.
 - To configure a configuration building block, select **Config > Global > All Building Blocks > building_block > Network > VLAN Interfaces**.
- 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.
- 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 immediately deploy this configuration. This option appears for virtual contexts.
 - OK** to save your entry. This option appears for configuration building blocks.
 - 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.
-

Related Topics

- [Configuring VLAN Interface Policy Map Use, page 9-7](#)
- [Configuring VLAN Interface Access Control, page 9-8](#)
- [Configuring VLAN Interface NAT Pools, page 9-10](#)
- [Configuring VLAN Interface Static ARP Entries, page 9-9](#)

Configuring Virtual Context BVI Interfaces

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



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

Procedure

- Step 1** Select the item to configure:
- To configure a virtual context, select **Config > Devices > context > Network > BVI Interfaces**.
 - To configure a configuration building block, select **Config > Global > All Building Blocks > building_block > Network > BVI Interfaces**.

The BVI Interface configuration table appears.

Step 2 Click **Add** to add a new BVI interface.

Step 3 Enter the interface attributes (see [Table 9-2](#)).

Table 9-2 BVI Interface Attributes

Field	Description
Bridge Group Number	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.
Admin Status	Indicate whether you want the interface to be up or down.

- Step 4** Click:
- Deploy Now** to immediately deploy this configuration. This option appears for virtual contexts.
 - OK** to save your entry. This option appears for configuration building blocks.
 - Cancel** to exit this procedure without saving your entries and to return to the previous table.
 - Next** to deploy your entries and to configure another BVI interface for this context.

Related Topics

- [Configuring Network Access, page 9-1](#)
- [Configuring Virtual Context Primary Attributes, page 3-11](#)

Viewing All BVI Interfaces by Context

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

The BVI Interface table appears with the information shown in [Table 9-3](#).

Table 9-3 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	Status of the interface, which can be up or down

Related Topics

- [Configuring VLAN Interfaces, page 9-2](#)
- [Using Virtual Contexts, page 3-1](#)
- [Configuring Virtual Context Primary Attributes, page 3-11](#)
- [Configuring VLAN Interfaces, page 9-2](#)
- [Configuring Virtual Context Syslog Settings, page 3-12](#)
- [Configuring Traffic Policies, page 11-1](#)

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 the item to configure:
- To configure a virtual context, select **Config > Devices > context > Network > Static Routes**.
 - To configure a configuration building block, select **Config > Global > All Building Blocks > building_block > Network > Static Routes**.

The Static Routes configuration table appears.

- Step 2** Click **Add** to add a new static route.



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 immediately deploy this configuration. This option appears for virtual contexts.
 - **OK** to save your entry. This option appears for configuration building blocks.
 - **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 static route.
-

Related Topics

- [Configuring Virtual Contexts, page 3-5](#)
- [Configuring Virtual Context Primary Attributes, page 3-11](#)

Viewing All Static Routes by Context

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

Procedure

-
- Step 1** Select **Config > Devices > 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 Port Channel Interfaces, page 9-21](#)
- [Configuring VLAN Interfaces, page 9-2](#)

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 > Devices > context** depend on the device associated with the virtual context and the role associated with your account.

Procedure

-
- Step 1** Select the item to configure:
- To configure a virtual context, select **Config > Devices > context > Network > Global IP DHCP**.
 - To configure a configuration building block, select **Config > Global > All Building Blocks > building_block > 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.
 - OK** to save your entry. This option appears for configuration building blocks.
 - 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.
-

Configuring Static VLANs for Over 8 K Static NAT Configurations



Note

This feature is for ACE 2.0 devices only.

Use this feature to create more than 8,000 static NAT configurations (one static NAT configuration with a netmask is counted as one configuration). In addition, take note of the following restrictions and requirements when using this feature:

- This feature is supported in routed mode only.
- Only one mapped interface is allowed per virtual context. However, each static NAT configuration must have a different mapped IP address.
- At any point, you can configure no more than one next-hop on the mapped interface.
- Bidirectional NAT, or in other words, source-address as well as destination-address translation, for the same flow is not supported.
- You must have less than 1,000 real IP addresses on the same subnet as the real interface. In addition, you must have less than 1,000 mapped IP address on the same subnet as the mapped interface.
- If you use this feature, we recommended you don't use MP-based NAT for the same virtual context.

Procedure

-
- Step 1** Select **Config > Devices > context > Network > Static NAT Overwrite**.
- The Static NAT Overwrite configuration table appears.
- Step 2** Click **Add** to add a new static NAT.
- Step 3** In the Mapped IP Addr field, enter the IP address to which the real IP address is translated. In a context, the mapped IP address must be different in each static NAT configuration.
- Step 4** In the Real VLAN number field, select the VLAN number of the interface connected to the real IP address network.
- Step 5** In the Mapped VLAN number field, select the VLAN number of the interface connected to the mapped IP address network. In a context, the mapped interface must be the same in each static NAT configuration.
- Step 6** In the Real IP address field, enter the real server IP address to be translated. In a context, you must configure a different address for configurations that have the same real server interface.
- Step 7** In the Real IP netmask field, enter the subnet mask for the real server address.
- Step 8** 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.
-

Configuring Gigabit Ethernet Interfaces



Note

This feature is for ACE appliances only.

The ACE appliance provides physical Ethernet ports to connect servers, PCs, routers, and other devices to the ACE appliance. The ACE appliance 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 appliance 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.
- **Access 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 appliance.

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

Procedure

-
- Step 1** Select **Config > Devices > context > Network > Gigabit Ethernet Interfaces**. The Physical Interface 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 9-4](#)).



Table 9-4 Physical Interface Attributes

Field	Description
Interface Name	Name of the gigabit interface, which is the <i>slot_number/port_number</i> where <i>slot_number</i> is the physical slot on the ACE for the specified port, and <i>port_number</i> 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 <ul style="list-style-type: none"> • Auto—Autonegotiate with other devices • 1000 Mbps • 100 Mbps • 10 Mbps

Table 9-4 *Physical Interface Attributes (continued)*

Field	Description
Duplex	<p>Specifies an interface duplex mode, which can be:</p> <ul style="list-style-type: none"> • 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.
Port Operation Mode	<p>Specifies the port operation mode, which can be:</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> – Port channel group number—Specify the port channel group number. – FT VLAN—Specify the fault tolerant (FT) VLAN used for communication between the members of the FT group. • Switchport—Specifies the interface switchport type: <ul style="list-style-type: none"> – 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: <ul style="list-style-type: none"> Trunk Native VLAN Trunk Allowed VLANs
FT Vlan	Specify the fault tolerant (FT) VLAN used for communication between the members of the FT group.

Table 9-4 Physical Interface Attributes (continued)

Field	Description
Carrier Delay	<p>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).</p> <hr/> <p> 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</p>
QoS Trust COS	<p>Enables Quality of Service (QoS) for the physical Ethernet port. By default, QoS is disabled for each physical Ethernet port on the ACE.</p> <p>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.</p> <p>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).</p> <hr/> <p> Note We recommend that you enable QoS on the FT VLAN port to provide higher priority for FT traffic.</p>

Step 4 Click:

- **Deploy Now** to immediately deploy this configuration.
- **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 VLAN Interfaces, page 9-2](#)
- [Configuring Virtual Context BVI Interfaces, page 9-12](#)
- [Configuring Port Channel Interfaces, page 9-21](#)

Configuring Port Channel Interfaces

**Note**

This feature is for ACE appliances only.

You can group physical ports together on the ACE appliance 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 a single port-channel interface only.

Step 1 Select **Config > Devices > context > Network > Port Channel Interfaces**. The Port Channel Interface 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 9-5](#)).

Table 9-5 Port Channel Interface Attributes

Field	Description
Port Channel 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.
FT 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.

Table 9-5 Port Channel Interface Attributes (continued)

Field	Description
ARP Inspection Type	<p>Instructs the ACE to check the source MAC address in an Ethernet header against the sender's MAC address in an ARP payload for every ARP packet received by the ACE on the specified interface. The ACE does not learn or update the ARP or MAC tables for packets with different MAC addresses. By default, source MAC validation is disabled.</p> <p>Note If ARP inspection fails, then the ACE does not perform source MAC validation.</p> <p>The options are as follows:</p> <ul style="list-style-type: none"> • N/A—Source MAC validation is disabled. • Flood—Enables ARP forwarding for the interface and forwards ARP packets with nonmatching source MAC addresses to all interfaces in the bridge group. This is the default option when you enable source MAC validation. • No-flood—Disables ARP forwarding for the interface and drops ARP packets with nonmatching source MAC addresses.

Table 9-5 Port Channel Interface Attributes (continued)

Field	Description
Load Balancing Method	<p>Specify one of the following load balancing methods:</p> <ul style="list-style-type: none"> • 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.
Switchport Type	<p>Specify the interface switchport type:</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> – Trunk Native VLAN – Trunk Allowed VLANs

Step 4 Click:

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

Related Topic

[Configuring VLAN Interfaces, page 9-2](#)

