CHAPTER 11

Configuring Network Access

Date: 9/23/10

This chapter describes how to configure network access using Cisco Application Networking Manager (ANM).

Note When naming ACE objects (such as a real server, virtual server, parameter map, class map, health probe, and so on), enter 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 are using ANM with an ACE module or ACE appliance and you configure a named object at the ACE CLI, keep in mind that ANM does not support all of the special characters that the ACE CLI allows you to use when configuring a named object. If you use special characters that ANM does not support, you may not be able to import or manage the ACE using ANM.

This chapter includes the following sections:

Information About VLANs

This section provides an overview of how the ACE module and appliance use VLANs.

This section includes the following topics:

- ACE Module VLANs, page 11-2
- ACE Appliance VLANs, page 11-2

ACE Module VLANs

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 engine to the ACE. After the VLANs are assigned to the ACE, you can configure the corresponding VLAN interfaces on the ACE as either routed or bridged 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 11-13.

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

Related Topics

- Configuring VLANs Using Cisco IOS Software (ACE Module), page 11-3
- Configuring VLAN Interfaces, page 11-5
- Configuring Virtual Context BVI Interfaces, page 11-13
- Configuring Virtual Context Static Routes, page 11-18
- Configuring Global IP DHCP, page 11-19

ACE Appliance VLANs

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 BVI with the bridge group.

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

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 11-5
- Configuring Virtual Context BVI Interfaces, page 11-13
- Configuring Gigabit Ethernet Interfaces on the ACE Appliance, page 11-21
- Configuring Port-Channel Interfaces for the ACE Appliance, page 11-24

Configuring VLANs Using Cisco IOS Software (ACE Module)

To allow the ACE module to receive traffic from the supervisor engine in the Catalyst 6500 series switch or Cisco 7600 series router, you must create VLAN groups on the supervisor engine and then assign the groups to the ACE module. After the VLAN groups are assigned to the ACE module, you can configure the VLAN interfaces on the ACE module. By default, all VLANs are allocated to the Admin context on the ACE module.

This section includes the following topics:

- Creating VLAN Groups Using Cisco IOS Software
- Assigning VLAN Groups to the ACE Module Through Cisco IOS Software
- Adding Switched Virtual Interfaces to the MSFC

Creating VLAN Groups Using Cisco IOS Software

In Cisco IOS software, you can create one or more VLAN groups and then assign the groups to the ACE module. For example, you can assign all the VLANs to one group, create an inside group and an outside group, or create a group for each customer.

You cannot assign the same VLAN to multiple groups; however, you can assign up to a maximum of 16 groups to an ACE. VLANs that you want to assign to multiple ACEs, for example, can reside in a separate group from VLANs that are unique to each ACE.

To assign VLANs to a group using Cisco IOS software on the supervisor engine, use the **svclc vlan-group** command. The syntax of this command is as follows:

svclc vlan-group *group_number vlan_range*

The arguments are as follows:

- *group_number*—Number of the VLAN group.
- *vlan_range*—One or more VLANs (2 to 1000 and 1025 to 4094) identified in one of the following ways:
  - A single number (*n*)
  - A range (*n-x*)

  Separate numbers or ranges by commas, as shown in this example:

  ```
  5,7-10,13,45-100
  ```

For example, to create three VLAN groups, 50 with a VLAN range of 55 to 57, 51 with a VLAN range of 75 to 86, and 52 with VLAN 100, enter:

```
Router(config)# svclc vlan-group 50 55-57
Router(config)# svclc vlan-group 51 70-86
```

```
Router(config)# svclc vlan-group 52 100
```

Related Topics

- Assigning VLAN Groups to the ACE Module Through Cisco IOS Software, page 11-4
- Adding Switched Virtual Interfaces to the MSFC, page 11-5

Assigning VLAN Groups to the ACE Module Through Cisco IOS Software

The ACE module cannot receive traffic from the supervisor engine unless you assign VLAN groups to it. To assign the VLAN groups to the ACE module using Cisco IOS software on the supervisor engine, use the **svc module** command in configuration mode. The syntax of this command is as follows:

svc module *slot_number* **vlan-group** *group_number_range*

The arguments are as follows:

- *slot_number*—Slot number where the ACE module resides. To display slot numbers and the devices in the chassis, use the **show module** command in Exec mode. The ACE module appears as the Application Control Engine Module in the Card Type field.
- *group_number_range*—One or more group numbers that are identified in one of the following ways:
  - A single number (*n*)
  - A range (*n-x*)

  Separate numbers or ranges by commas, as shown in this example:

  ```
  5,7-10
  ```

For example, to assign VLAN groups 50 and 52 to the ACE module in slot 5, and VLAN groups 51 and 52 to the ACE module in slot 8, enter:

```
Router(config)# svc module 5 vlan-group 50,52
Router(config)# svc module 8 vlan-group 51,52
```

To view the group configuration for the ACE module and the associated VLANs, use the **show svclc vlan-group** command. For example, enter:

```
Router(config)# exit
Router# show svclc vlan-group
```

To view VLAN group numbers for all devices, use the **show svc module** command. For example, enter:

```
Router# show svc module
```

Note Enter the **show vlans** command in Exec mode from the Admin context to display the ACE module VLANs that are downloaded from the supervisor engine.

Related Topics

- Creating VLAN Groups Using Cisco IOS Software, page 11-3
- Adding Switched Virtual Interfaces to the MSFC, page 11-5

Adding Switched Virtual Interfaces to the MSFC

A VLAN defined on the Multilayer Switch Feature Card (MSFC) is called a switched virtual interface (SVI). If you assign the VLAN used for the SVI to the ACE module, then the MSFC routes between the ACE module and other Layer 3 VLANs. By default, only one SVI can exist between the MSFC and the ACE. However, for multiple contexts, you may configure multiple SVIs for unique VLANs on each context.

Procedure:

Step 1 (Optional) If you need to add more than one SVI to the ACE module, enter the following command:

```
Router(config)# svclc multiple-vlan-interfaces
```

Step 2 Add a VLAN interface to the MSFC. For example, to add VLAN 55, enter the following command:

```
Router(config)# interface vlan 55
```

Step 3 Set the IP address for this interface on the MSFC. For example, to set the address 10.1.1.1 255.255.255.0, enter the following command:

```
Router(config-if)# ip address 10.1.1.1 255.255.255.0
```

Step 4 Enable the interface. For example, enter the following command:

```
Router(config-if)# no shut
```

Note To monitor any VLAN that is associated with more than two trunk ports, physical ports, or trunk-physical ports on the supervisor engine, enable the autostate feature by using the **svclc autostate** command. When you associate a VLAN to these ports, autostate declares that the VLAN is up. When a VLAN state change occurs on the supervisor engine, autostate sends a notification to the ACE module to bring the interface up or down.

To view this SVI configuration, use the **show interface vlan** command. For example, enter:

```
Router# show int vlan 55
```

Related Topics

- Creating VLAN Groups Using Cisco IOS Software, page 11-3
- Assigning VLAN Groups to the ACE Module Through Cisco IOS Software, page 11-4

Configuring VLAN Interfaces

You can configure VLAN interfaces for virtual contexts on the ACE.

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

Assumptions

This topic assumes the following:

- A Layer 3/Layer 4 or Management policy map has been configured for this virtual context. For more information, see Configuring Traffic Policies, page 13-1.
- 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 5-74.

Procedure

Step 1 Choose the item to configure:

- To configure a virtual context, choose **Config** > **Devices** > *context* > **Network** > **VLAN Interfaces**.
- To configure a configuration building block, choose **Config** > **Global** > **All Building Blocks** > *building_block* > **Network** > **VLAN Interfaces**.

The VLAN Interface table appears.

Step 2 In the VLAN Interface table, click **Poll Now** to instruct ANM to poll the devices and display the current values and click **OK** when prompted if you want to poll the devices for data now.

Step 3 Click **Add** to add a new VLAN interface, or choose an existing VLAN interface and click **Edit** to modify it.

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

Step 4 Enter the VLAN interface attributes (see Table 11-1). Click **More Settings** to access the additional VLAN interface attributes.

By default, ANM hides the default VLAN interface attributes and the VLAN interface attributes that are not commonly used.

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

Table 11-1 VLAN Interface Attributes

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

Table 11-1 VLAN Interface Attributes (continued)

Field	Description
Interface Type	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	Field that appears for the Routed Interface Type. Enter the IP address assigned to this interface.
Alias IP Address	Field that appears for the Routed Interface Type. Enter the IP address of the alias that this interface is associated with.
Peer IP Address	Field that appears for the Routed Interface Type. Enter the IP address of the remote peer.
Netmask	Field that appears for the Routed Interface Type. Choose the subnet mask to be used.
BVI	Field that appears for the Bridged Interface Type. Enter the number of the bridge group to be configured on this VLAN. When you configure a bridge group on a VLAN, the ACE automatically makes it bridged. Valid entries are from 1 to 4094.
Admin Status	Administrative state of the interface. Specify whether you want the interface to be Up or Down.
Enable MAC Sticky	Check box that instructs the ACE to convert dynamic MAC addresses to sticky secure MAC addresses and to add this information to the running configuration. Uncheck the check box to indicate that the ACE is not to convert dynamic MAC addresses to sticky secure MAC addresses.
Enable Normalization	Check box that specifies that normalization is to be enabled on this interface. Uncheck the check box to indicate that normalization is to be disabled on this interface. ⚠ **Caution** Disabling normalization may expose your ACE 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 11-1 VLAN Interface Attributes (continued)

Field	Description
More Settings	
Secondary IP Groups	Option that is available only for the ACE module A2(3.0), ACE appliance A4(1.0), and later releases of both device types. This option displays only when Interface Type is set to Routed. The number of secondary IP groups that you can enter for a VLAN depends on the ACE release as follows: • ACE module A2(3.0) and ACE appliance A4(1.0)—Up to 4 secondary IP groups. • ACE module A2(3.1) and later—Up to 15 secondary IP groups. 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 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 the first two steps 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 11-1 VLAN Interface Attributes (continued)

Field	Description
ARP Inspection Type	Type of ARP inspection, which 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. 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. **Note** If ARP inspection fails, then the ACE does not perform source MAC validation. Choices 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 setting is the default. 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	Maximum number of fragments that belong to the same packet that the ACE is to accept for reassembly. Valid entries are from 1 to 256. The default is 112.
Min. Fragment MTU Value	Minimum Maximum Transmission Units (MTUs) for each allowable fragment. Valid entries are from 28 to 9216 with no default.
MTU Value	Number of bytes for MTU). Valid entries are from 68 to 9216. The default is 1500.
Reassembly Timeout (Seconds)	Number of seconds that the ACE is to wait before it abandons the fragment reassembly process if it does not receive any outstanding fragments for the current fragment chain (that is, fragments that belong to the same packet). Valid entries are 1 to 30 seconds.
Reverse Path Forwarding (RPF)	Check box that instructs the ACE to discard IP packets if no reverse route is found or if the route does not match the interface on which the packets arrived. Uncheck the check box to indicate that the ACE is not to filter or discard packets based on the ability to verify the source IP address.
Enable MAC Address Autogenerate	MAC address autogenerate option, which allows you to configure a different MAC address for the VLAN interface.
Enable ICMP Guard	Check box that enables ICMP Guard on the ACE. Uncheck the check box to specify that ICMP Guard is not to be enabled on ACE. **Caution** Disabling ICMP security checks may expose your ACE and network to potential security risks. When you disable ICMP Guard, the ACE no longer performs NAT translations on the ICMP header and payload in error packets, which can potentially reveal real host IP addresses to attackers.

Table 11-1 VLAN Interface Attributes (continued)

Field	Description
Enable DHCP Relay	Check box that instruct the ACE to accept DHCP requests from clients on this interface and to enable the DHCP relay agent. Uncheck the check box to specify that the ACE is not to accept DHCP requests or enable the DHCP relay agent.
Action For DF Bit	Action that the ACE takes when a packet has its DF (Don't Fragment) bit set in the IP header: • **Allow**—The ACE permits the packet with the DF bit set. If the packet is larger than the next-hop MTU, ACE discards the packet and sends an ICMP unreachable message to the source host. • **Clear**—The ACE clears the DF bit and permit the packet. If the packet is larger than the next-hop MTU, the ACE fragments the packet.
Action For IP Header Options	Action that the ACE takes when an IP option is set in a packet: • **Allow**—The ACE allows the IP packet with the IP options set. • **Clear**—The ACE clears all IP options from the packet and to allow the packet. • **Clear-Invalid**—The ACE clears the invalid IP options from the packet and then allow the packet. • **Drop**—The ACE discards the packet regardless of any options that are set.
Min. TTL IP Header Value	Minimum number of hops that a packet is allowed to reach its destination. Valid entries are from 1 to 255. Each router along the path decrements the TTL by one. If the packet 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 from 2 to 65535.
UDP Config Commands	UDP boost command options: • **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	Policy map that is associated with this VLAN interface. From the Available list, double-click a policy map name 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	ACL input access group to be associated with this VLAN interface. From the Available list, double-click an ACL name 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	ACL output access group that is associated with this VLAN interface. From the Available list, double-click an ACL name 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.

Table 11-1 VLAN Interface Attributes (continued)

Field	Description
Static ARP Entry (IP/MAC Address)	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	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 Do one of the following:

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

Step 6 (Optional) To display statistics and status information for a VLAN interface, choose the VLAN interface from the VLAN Interface table, then click **Details**.

The **show interface vlan** CLI command output appears. See the "Displaying VLAN Interface Statistics and Status Information" section on page 11-12 for details.

Related Topics

- Configuring VLAN Interface NAT Pools, page 11-16
- Displaying All VLAN Interfaces, page 11-11
- Displaying VLAN Interface Statistics and Status Information, page 11-12

Displaying All VLAN Interfaces

You can display all of the VLAN interfaces associated with a specific virtual context by choosing **Config > Devices** > *context* > **Network > VLAN Interfaces**.

The VLAN Interface table appears with the information shown in Table 11-2.

Table 11-2 VLAN Interface Table Fields

Field	Description
VLAN	VLAN number.
Description	Description for this interface.
Interface Type	Role of the virtual context in the network topology of the VLAN interface.
IP Address	IP address assigned to this interface.
Netmask	Subnet mask for this interface.
BVI	Bridged group number.
Admin Status	Status of the interface, which can be Up or Down.
Operational Status	Operational state of the device (Up or Down).
Last Polled	Date and time of the last time that ANM polled the device to display the current values.

Related Topics

- Configuring VLAN Interfaces, page 11-5
- Configuring Virtual Context BVI Interfaces, page 11-13
- Displaying VLAN Interface Statistics and Status Information, page 11-12

Displaying VLAN Interface Statistics and Status Information

You can display statistics and status information for a particular VLAN interface.

Procedure

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

The VLAN Interfaces table appears.

Step 2 Choose a VLAN interface from the VLAN Interfaces table, and click **Details**.

The **show interface vlan** CLI command output appears. For details on the displayed output fields, see either the *Cisco ACE Module Routing and Bridging Configuration Guide* or the *Cisco ACE 4700 Series Appliance Routing and Bridging Configuration Guide*.

Step 3 Click **Update Details** to refresh the output for the **show interface vlan** CLI command.

Step 4 Click **Close** to return to the VLAN Interfaces table.

Related Topics

- Configuring VLAN Interfaces, page 11-5
- Displaying All VLAN Interfaces, page 11-11

Configuring Virtual Context BVI Interfaces

You can configure Bridge-Group Virtual Interfaces (BVI) for virtual contexts. The ACE supports virtual contexts containing BVI interfaces. 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 Layer 2 VLANs per bridge group.

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

This section includes the following topics:

- Configuring BVI Interfaces for a Virtual Context., page 11-13
- Displaying All BVI Interfaces by Context, page 11-15
- Displaying BVI Interface Statistics and Status Information, page 11-15

Configuring BVI Interfaces for a Virtual Context.

Procedure

Step 1 Choose the item to configure:

- To configure a virtual context, choose **Config > Devices >** *context* **> Network > BVI Interfaces**.
- To configure a configuration building block, choose **Config > Global > All Building Blocks >** *building_block* **> Network > BVI Interfaces**.

The BVI Interface configuration table appears.

Step 2 Click **Poll Now** to instruct ANM to poll the devices and display the current values, and click **OK** when prompted if you want to poll the devices for data now.

Step 3 Click **Add** to add a new BVI interface.

Step 4 Enter the interface attributes (see Table 11-3).

Note When you create or edit a virtual context BVI, if either of the two VLANs do not exist, ANM creates the VLAN and populates the BVI with the description specified in the BVI Interface window.

If you delete the BVI and there are values specified in either of the two VLAN fields, ANM removes the BVI value from the VLAN.

Table 11-3 BVI Interface Attributes

Field	Description
BVI	BVI identifier. Either accept the automatically incremented entry or enter a different, unique value for the BVI. Valid entries are from 1 to 4094.
Description	Brief description for this interface.
IP Address	IP address assigned to this interface.

Table 11-3 BVI Interface Attributes (continued)

Field	Description
Alias IP Address	IP address of the alias that this interface is associated with.
Peer IP Address	IP address of the remote peer.
Netmask	Subnet mask to be used.
Admin Status	Administrative state of the interface: **Up** or **Down**.
Secondary IP Groups	Option that is available only for the ACE module A2(3.0), ACE appliance A4(1.0), and later releases of either device type. The number of secondary IP groups that you can enter for a BVI depends on the ACE release as follows: • ACE module A2(3.0) and ACE appliance A4(1.0)—Up to 4 secondary IP groups. • ACE module A2(3.1) and later—Up to 15 secondary IP groups. To create 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 the first two steps 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	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	Brief 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. Valid entries are from 2 to 4094.
Second VLAN Description	Brief description for the second VLAN.

Step 5 Do one of the following:

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

Step 6 To display statistics and status information for a BVI interface, choose the BVI interface from the BVI Interface table, and click **Details**.

The **show interface bvi** CLI command output appears. See the "Displaying BVI Interface Statistics and Status Information" section on page 11-15 for details.

Related Topics

- Configuring Network Access, page 11-1
- Configuring Virtual Context Primary Attributes, page 5-12

Displaying All BVI Interfaces by Context

You can display all of the BVI interfaces associated with a specific context by choosing **Config > Devices > *context* > Network > BVI Interfaces**.

The BVI Interface table appears with the information shown in Table 11-4.

Table 11-4 BVI Interface Fields

Field	Description
BVI	Name of the BVI interface.
Description	Description for the BVI 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.
Operational Status	Operational state of the device (Up or Down).
Last Polled	Date and time of the last time that ANM polled the device to display the current values.
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

- Displaying BVI Interface Statistics and Status Information, page 11-15

Displaying BVI Interface Statistics and Status Information

You can display statistics and status information for a particular BVI interface by using the **Details** button. ANM accesses the **show interface bvi** CLI command to display detailed BVI interface information.

Procedure

Step 1 Choose **Config** > **Devices** > *context* > **Network** > **BVI Interfaces**.

The BVI Interface table appears.

Step 2 In the BVI Interface table, choose a BVI interface from the BVI Interface table, and click **Details**.

The **show interface bvi** CLI command output appears. For details on the displayed output fields, see either the *Cisco ACE Module Routing and Bridging Configuration Guide* or the *Cisco ACE 4700 Series Appliance Routing and Bridging Configuration Guide*.

Step 3 Click **Update Details** to refresh the output for the **show interface bvi** CLI command.

Step 4 Click **Close** to return to the BVI Interface table.

Related Topics

- Displaying All BVI Interfaces by Context, page 11-15

Configuring VLAN Interface NAT Pools

You can configure Network Address Translation (NAT) pools for a VLAN interface. 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 allows you to configure NAT so that it advertises only one address for the entire network to the outside world. This feature, which effectively hides the entire internal network behind that address, offers 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.

Note The options that appear when you choose 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 11-5).

Procedure

Step 1 Choose the item to configure:

- To configure a virtual context, choose **Config** > **Devices** > *context* > **Network** > **NAT Pools**.
- To configure a configuration building block, choose **Config** > **Global** > **All Building Blocks** > *building_block* > **Network** > **NAT Pools**.

The NAT Pools table appears.

Step 2 In the NAT Pools table, click **Add** to add a new NAT pool, or choose an existing NAT pool and click **Edit** to modify it.

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

Step 3 Choose the VLAN interface that you want to configure a NAT pool for and click the **NAT Pool** tab.

The NAT Pool configuration table appears.

Step 4 In the NAT Pool configuration table, click **Add** to add a new entry.

Step 5 In the VLAN ID field, from the drop-down list, choose a VLAN entry.

Step 6 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 from 1 to 2147483647.

Step 7 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 8 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 9 In the Netmask field, choose the subnet mask for the global IP addresses in the NAT pool.

Step 10 Check the PAT Enabled check box to instruct the ACE to perform port address translation (PAT) in addition to NAT.

Uncheck the check box to indicate that the ACE is not to perform port address translation (PAT) in addition to NAT.

Step 11 Do one of the following:

- Click **Deploy Now** to immediately deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files. This option appears for virtual contexts.
- Click **OK** to save your entry. This option appears for configuration building blocks.
- Click **Cancel** to exit this procedure without saving your entries and to return to the NAT Pools table.
- Click **Next** to deploy your entries and to add another NAT Pool entry.

Related Topics

- Configuring VLAN Interfaces, page 11-5
- Configuring Virtual Context BVI Interfaces, page 11-13

Configuring Virtual Context Static Routes

Note This functionality is available for Admin virtual contexts only.

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

Procedure

Step 1 Choose the item to configure:

- To configure a virtual context, choose **Config > Devices >** *context* **> Network > Static Routes**.
- To configure a configuration building block, choose **Config > Global > All Building Blocks >** *building_block* **> Network > Static Routes**.

The Static Routes configuration table appears.

Step 2 In the Static Routes configuration table, 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 that you specify for the static route is the address that is in the packet before entering the ACE 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, choose 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.

Step 6 The gateway address must be in the same network as a VLAN interface for this context.

Step 7 Do one of the following:

- Click **Deploy Now** to immediately deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files. This option appears for virtual contexts.
- Click **OK** to save your entry. This option appears for configuration building blocks.
- Click **Cancel** to exit this procedure without saving your entries and to return to the previous table.
- Click **Next** to deploy your entries and to add another static route.

Related Topics

- Configuring Virtual Contexts, page 5-7
- Configuring Virtual Context Primary Attributes, page 5-12

Displaying All Static Routes by Context

You can display all of the static routes associated with a context by choosing **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 for the ACE Appliance, page 11-24
- Configuring VLAN Interfaces, page 11-5

Configuring Global IP DHCP

You can configure the Dynamic Host Configuration (DHCP) relay agent at the context level so the configuration applies to all interfaces associated with the context. 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.

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

Procedure

Step 1 Choose the item to configure:

- To configure a virtual context, choose **Config > Devices >** *context* **> Network > Global IP DHCP**.
- To configure a configuration building block, choose **Config > Global > All Building Blocks >** *building_block* **> Network > Global IP DHCP**.

The Global IP DHCP configuration table appears.

Step 2 In the Global IP DHCP configuration table, click **Enable DHCP Relay For The Context** to enable DHCP relay for the context and all interfaces associated with this context.

Step 3 In the Relay Agent Information Reforwarding Policy field, choose a relay agent information forwarding policy:

- **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, choose the IP DHCP server to which the DHCP relay agent is to forward client requests.

Step 5 Do one of the following:

- Click **Deploy Now** to immediately deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files. This option appears for virtual contexts.
- Click **OK** to save your entry. This option appears for configuration building blocks.
- Click **Cancel** to exit this procedure without saving your entries and to return to the previous table.
- Click **Next** to deploy your entries and to add another DHCP relay entry.

Configuring Static VLANs for Over 8000 Static NAT Configurations

Note This feature is for ACE modules only.

You can create more than 8,000 static NAT configurations (one static NAT configuration with a netmask is counted as one configuration). In addition, follow these restrictions and guidelines 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 fewer than 1,000 real IP addresses on the same subnet as the real interface. In addition, you must have fewer than 1,000 mapped IP address on the same subnet as the mapped interface.
- If you use this feature, we recommended that you do not use MP-based NAT for the same virtual context.

Procedure

Step 1 Choose **Config > Devices >** *context* **> Network > Static NAT Overwrite**.

The Static NAT Overwrite configuration table appears.

Step 2 In the Static NAT Overwrite configuration table, click **Add** to add a new static NAT.

Step 3 In the Mapped IP Address 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, choose the VLAN number of the interface connected to the real IP address network.

Step 5 In the Mapped VLAN Number field, choose the VLAN number of the interface connected to the mapped IP address network.

Step 6 In a context, the mapped interface must be the same in each static NAT configuration.

Step 7 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 8 In the Real IP Netmask field, enter the subnet mask for the real server address.

Step 9 Do one of the following:

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

Configuring Gigabit Ethernet Interfaces on the ACE Appliance

Note This feature is for ACE appliances only.

You can configure a Gigabit Ethernet interface on the ACE appliance, which 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 follows:

- 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.

This section includes the following topics:

- Configuring Gigabit Ethernet Interfaces, page 11-21
- Displaying Gigabit Ethernet Interface Statistics and Status Information, page 11-24

Configuring Gigabit Ethernet Interfaces

This section describes how to configure Gigabit Interfaces on the ACE.

Procedure

Step 1 Choose **Config > Devices >** *context* **> Network > GigabitEthernet Interfaces**.

The GigabitEthernet Interfaces table appears.

Step 2 In the GigabitEthernet Interfaces table, click **Poll Now** to instruct ANM to poll the devices and display the current values, and click **OK** when prompted to poll the devices for data.

Step 3 Choose an existing gigabit Ethernet interface, and click **Edit** to modify it.

Step 4 Enter the gigabit Ethernet physical interface attributes (see Table 11-5).

Table 11-5 Physical Interface Attributes

Field	Description
Interface Name	Name of the Gigabit Ethernet interface, which is in the format *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	Brief description for this interface.
Admin Status	Administrative state of the interface: **Up** or **Down**.
Speed	Port speed: • **Auto**—Autonegotiate with other devices • **10 Mbps** • **100 Mbps** • **1000 Mbps**
Duplex	Interface duplex mode: • **Auto**—Resets the specified Ethernet port to automatically negotiate port speed and duplex of incoming signals. This is the default setting. • **Full**—Configures the specified Ethernet port for full-duplex operation, which allows data to travel in both directions at the same time. • **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.
Port Operation Mode	Port operation mode: • **N/A**—Specifies 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—Specifies the port channel group number. • HA VLAN—Specifies the high availability (HA) VLAN used for communication between the members of the FT group. • **Switch Port**—Specifies the interface switch port 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 choose 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 allocates individual VLANs to a trunk link.

Table 11-5 Physical Interface Attributes (continued)

Field	Description
HA LAN	High availability (HA) VLAN used for communication between the members of the FT group.
Carrier Delay	Configurable delay at the physical port level to address any issues with transition time, based on the variety of peers. Valid values are from 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 switch 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 does not pass. In this case, you should specify a carrier delay.
QoS Trust COS	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 is based on VLAN Class 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 5 Do one of the following:

- Click **Deploy Now** to immediately deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.
- Click **Cancel** to exit the procedure without saving your changes and to return to the Physical Interface table.
- Click **Next** or **Previous** to go to the next or previous physical channel.
- Click **Delete** to remove this entry from the Physical Interface table and to return to the table.

Step 6 (Optional) To display statistics and status information for a particular Gigabit Ethernet interface, choose the interface from the GigabitEthernet Interfaces table, and click **Details**.

The **show interface gigabitEthernet** CLI command output appears. See the "Displaying Gigabit Ethernet Interface Statistics and Status Information" section on page 11-24 for details.

Related Topics

- Configuring VLAN Interfaces, page 11-5
- Configuring Virtual Context BVI Interfaces, page 11-13
- Configuring Port-Channel Interfaces for the ACE Appliance, page 11-24

Displaying Gigabit Ethernet Interface Statistics and Status Information

You can display statistics and status information for a particular Gigabit Ethernet interface.

Procedure

Step 1 Choose **Config > Devices** > *context* **> Network > GigabitEthernet Interfaces**.

The GigabitEthernet Interfaces table appears.

Step 2 In the GigabitEthernet Interfaces table, choose a Gigabit Ethernet interface from the GigabitEthernet Interfaces table, and click **Details**.

The **show interface gigabitEthernet** CLI command output appears. For details on the displayed output fields, see the *Cisco ACE 4700 Series Appliance Routing and Bridging Configuration Guide*.

Step 3 (Optional) Click **Update Details** to refresh the display.

Step 4 Click **Close** to return to the GigabitEthernet Interfaces table.

Related Topics

Configuring Gigabit Ethernet Interfaces on the ACE Appliance, page 11-21

Configuring Port-Channel Interfaces for the ACE Appliance

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

- Why Use Port Channels?, page 11-24
- Configuring a Port-Channel Interface, page 11-25
- Configuring a Catalyst 6500 for an ACE Appliance Port-Channel Interface Connection, page 11-27
- Displaying Port Channel Interface Statistics and Status Information, page 11-29

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:

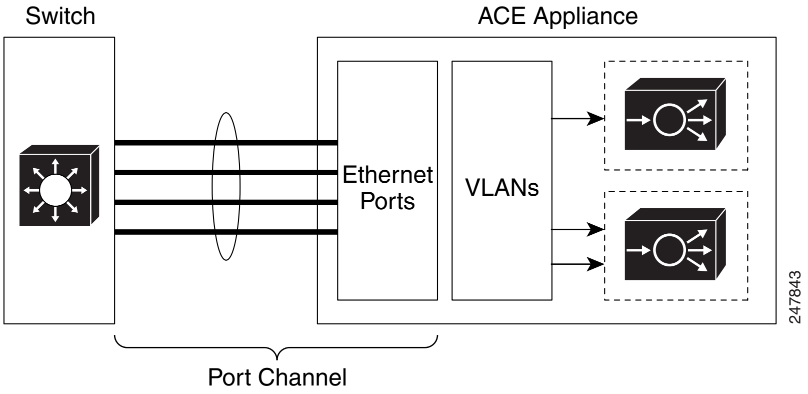
- Improves link reliability through physical redundancy.
- Allows greater total throughput to the ACE appliance. For example, four 1-GigaBit Ethernet interfaces can be aggregated into a single 4 GigaBit channel.
- Allows traffic capacity to be scaled up in the future, without network disruption at that 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. For an example of how to configure a Cisco Catalyst 6500 switch to enable a port channel connection to ACE, see the "Configuring a Catalyst 6500 for an ACE Appliance Port-Channel Interface Connection" section on page 11-27.

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 11-1illustrates a port channel interface.

Figure 11-1 Example of a Port Channel Interface



Related Topic

Configuring a Port-Channel Interface, page 11-25

Displaying Port Channel Interface Statistics and Status Information, page 11-29

Configuring a Port-Channel Interface

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 Choose **Config** > **Devices** > *context* > **Network** > **Port Channel Interfaces**.

The Port Channel Interface table appears.

Step 2 In the Port Channel Interface table, click **Poll Now** to instruct ANM to poll the devices and display the current values, and click **OK** when prompted to poll the devices for data.

Step 3 Click **Add** to add a port channel interface, or choose an existing port channel interface and click **Edit** to modify it.

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

Step 4 Enter the port channel interface attributes (see Table 11-6).

Table 11-6 Port Channel Interface Attributes

Field	Description
Interface Number	Channel number for the port-channel interface, which can be from 1 to 255.
Description	Brief description for this interface.
Fault Tolerant VLAN	Fault tolerant (FT) VLAN used for communication between the members of the FT group.
Admin Status	Administrative state of the interface: **Up** or **Down**.
Load Balancing Method	Load balancing method: • **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.
Switch Port Type	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 choose 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 5 Do one of the following:

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

Step 6 (Optional) To display statistics and status information for a particular port-channel interface, choose the interface from the Port Channel Interfaces table, and click **Details**.

The **show interface port-channel** CLI command output appears. See the "Displaying Port Channel Interface Statistics and Status Information" section on page 11-29 for details.

Related Topic

Configuring Port-Channel Interfaces for the ACE Appliance, page 11-24

Configuring Port-Channel Interfaces for the ACE Appliance, page 11-24

Displaying Port Channel Interface Statistics and Status Information, page 11-29

Configuring VLAN Interfaces, page 11-5

Configuring a Catalyst 6500 for an ACE Appliance Port-Channel Interface Connection

This section provides information for you to configure a port-channel interface on a network device such as the Cisco Catalyst 6500. After you configure the port channels for the ACE appliance through ANM and you physically connect the Gigabit Ethernet physical interfaces on the ACE appliance to the Catalyst 6500 switch ports, configure the port channels on the switch. The information outlined in this topic is intended as an example of configuring port channels on a switch. You can adapt this information for whatever switch the ACE appliance is connected to in your network.

For specific details on configuring the Cisco Catalyst 6500, see the documentation set on www.Cisco.com.

This section includes the following topics:

- Creating the Port Channel Interface on the Catalyst 6500
- Adding Interfaces to the Port Channel

Creating the Port Channel Interface on the Catalyst 6500

This section contains and example in which a Cisco Catalyst 6500 is configured with a port channel using an 802.1q trunk that allows the associated VLANs. The native VLAN of the trunk is VLAN 10.

Note Default VLAN 1 should not be used for the native VLAN because this VLAN is used internally on the ACE appliance.

Port-channel load balancing is used to distribute the traffic load across each of the links in the port channel to ensure efficient utilization of each link. Port-channel load balancing on the Cisco Catalyst 6500 can use MAC addresses or IP addresses, Layer 4 port numbers, source addresses, destination addresses, or both source and destination addresses. By default, the ACE appliance uses Src-Dst-MAC to make a load balancing decision (see Table 11-6). The recommended best practice is to use the source and destination Layer 4 port for the load balancing decision.

The following example illustrates the CLI commands used to configure a port channel interface for the Cisco Catalyst 6500:

```
Switch(config)# port-channel load-balance src-dst-port
Switch(config)# interface port-channel 1
Switch(config-if)# description For Connection with ACE Appliance
Switch(config-if)# switchport
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport trunk native vlan 10
Switch(config-if)# switchport trunk allowed vlan 10,20,30,31, 40,50
Switch(config-if)# switchport nonegotiate
Switch(config-if)# mls qos trust cos
```

After you configure the port channel on the Cisco Catalyst 6500, you can then add it to the configuration of the four interfaces as described in the "Adding Interfaces to the Port Channel" section on page 11-28.

Note The ACE appliance does not support Port Aggregation Protocol (PAgP) or Link Aggregate Control Protocol (LACP) so the port-channel interface is configured using **mode on**.

Adding Interfaces to the Port Channel

The following example illustrates the CLI commands used to configure the four switch ports 3/9 through 3/12 as members of the port channel on the Cisco Catalyst 6500:

```
Switch(config-if)# int range Gig 3/9 - 12
Switch(config-if-range)# channel-group 1 mode on
Switch(config-if-range)# speed 1000
Switch(config-if-range)# spanning-tree portfast trunk
Switch(config-if-range)# no shut
```

On the ACE appliance, you can configure the Ethernet port speed for a setting of 10, 100, or 1000 Mbps by configuring the Speed field for a Gigabit Ethernet physical interface attributes (see Table 11-5). The default for the ACE appliance is the auto-negotiate interface speed. We recommend that you configure the speed to 1000 on both the Cisco Catalyst 6500 and the ACE appliance to avoid relying on auto negotiation of the interface speed. A speed setting of 1000 helps to avoid the possibility of the interface operating below the expected Gigabit speed and ensures that the port-channel interface reaches the maximum 4 Gbps throughput.

The ACE appliance does not implement Spanning-Tree protocol and does not take part in Spanning-Tree root bridge election process. PortFast is configured on the Cisco Catalyst 6500 to reduce the time required for spanning tree to allow traffic on the port connected to the ACE interface by immediately moving to the forwarding state, bypassing the block, listening, and learning states. The average time for switch port moving into a forward state is approximately 30 seconds. Using PortFast reduces this time to approximately 5 seconds.

Note In virtual partitions operating in bridge mode, the ACE offers an option to bridge Spanning-Tree BPDUs between two VLANs to prevent the possibility of a loop. Such a loop may occur when two partitions actively forward traffic. This should not happen during normal operation; however, the option to bridge BPDUs provides a safeguard against this condition. Upon detecting BPDUs, the switch connected to the ACE appliance immediately blocks the port/VLAN from which the loop originated from. We recommend that you configure an ethertype ACL that includes the BPDU protocol and apply the ACL to Layer 2 interfaces in bridge mode.

Displaying Port Channel Interface Statistics and Status Information

You can display statistics and status information for a particular port-channel interface.

Procedure

Step 1 Choose **Config** > **Devices** > *context* > **Network** > **Port Channel Interfaces**.

The Port Channel Interfaces table appears.

Step 2 In the Port Channel Interfaces table, choose a port-channel interface from the Port Channel Interfaces table, and click **Details**.

The **show interface port-channel** CLI command output appears. For details about the displayed output fields, see the *Cisco ACE 4700 Series Appliance Routing and Bridging Configuration Guide*.

Step 3 (Optional) Click **Update Details** to refresh the display.

Step 4 Click **Close** to return to the Port Channel Interfaces table.

Related Topics

Configuring Port-Channel Interfaces for the ACE Appliance, page 11-24