CHAPTER 3

Using ANM Guided Setup

Date: 9/23/10

This chapter describes how to use Cisco Application Networking Manager (ANM) Guided Setup.

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 Guided Setup

ANM Guided Setup provides a series of setup sequences that offer GUI window guidance and networking diagrams to simplify the configuration of ANM and the network devices that it mananges.

Guided Setup allows you to quickly perform the following tasks:

- Establish communication between ANM and Application Control Engine (ACE) hardware devices.
- Configure ACE devices that are new to the network by establishing network connectivity in either standalone or high-availability (HA) deployments.
- Create and connect to an ACE virtual context.
- Set up load balancing application from an ACE to a group of back-end servers.

To access Guided Setup, click the Config tab located at the top of the window, then click Guided Setup.

Note The available menu and button options on the Guided Setup tasks are under Role-Based Access Control (RBAC). Menu and button options will be grayed if proper permission has not been granted to the logged in user by the administrator. See the "How ANM Handles Role-Based Access Control" section on page 17-8 for more information about RBAC in ANM.

Table 3-1 identifies the individual guided setup tasks and related topics.

Table 3-1 Guided Setup Tasks and Related Topics

Guided Setup Tasks	Purpose	Related Topics
Import devices	Launch the Import Devices setup task to establish communication between ANM and hardware devices. Imported devices can include: ACE modules, ACE appliances, Catalyst 6500 series chassis, Catalyst 6500 Virtual Switching System (VSS) 1440, Cisco 7600 series routers, Content Services Switches (CSS) devices, Content Switching Module (CSM) devices, or Global Site Selector (GSS) devices.	• Using Import Devices, page 3-3 • Information About Importing Devices, page 4-3 • Preparing Devices for Import, page 4-4 • Importing Network Devices into ANM, page 4-9 • Discovering Large Numbers of Devices Using IP Discovery, page 4-25
ACE hardware setup	Launch the ACE Hardware Setup task to help you configure ACE devices that are new to the network by establishing network connectivity in either standalone or high-availability (HA) deployments.	• Using ACE Hardware Setup, page 3-4 • Configuring Devices, page 4-32 • Configuring ACE Module and Appliance Role-Based Access Controls, page 4-51 • Managing Devices, page 4-64 • Configuring ACE High Availability Peers, page 12-14
Virtual context setup	Launch the Virtual Context Setup task to create and connect an ACE virtual context.	• Using Virtual Context Setup, page 3-9 • Using Resource Classes, page 5-41 • Creating Virtual Contexts, page 5-2 • Configuring Virtual Contexts, page 5-7 • Configuring VLANs Using Cisco IOS Software (ACE Module), page 11-3
Application setup	Launch the Application Setup task to configure load balancing for your application. This task guides you through a complete end-to-end configuration of the ACE for many common server load-balancing situations.	• Using Application Setup, page 3-11 • Configuring VLAN Interfaces, page 11-5 • Configuring Virtual Context BVI Interfaces, page 11-13 • Configuring Virtual Context Static Routes, page 11-18 • Configuring Virtual Context BVI Interfaces, page 11-13 • Configuring Security with ACLs, page 5-74 • SSL Setup Sequence, page 10-4

Guidelines and Limitations

As you perform a Guided Setup task, use the following operating conventions:

- To move between steps, click the name of the step in the menu to the left.
- The steps for each task are listed in an order that is designed to prevent problems during later steps; however, you can skip steps if you know they are not applicable to your application.
- Depending on your user privileges, ANM may prevent you from making changes on certain steps.
- You must save and deploy any changes you want to keep before leaving each page.
- Each task can be run as many times as you like.

Using Import Devices

You can use the Import Device task to import ACE modules, ACE appliances, Catalyst 6500 series chassis, Catalyst 6500 Virtual Switching System (VSS) 1440, Cisco 7600 series routers, CSS devices, CSM devices, or GSS devices into ANM. You must import the hardware devices before ANM can manage them.

Before You Begin

- Because ANM communicates with network devices through Secure Shell (SSH) and other protocols, you must set up your devices to allow ANM to collect data from them. See the "Preparing Devices for Import" section on page 4-4.
- Before ANM can import a device, you must ensure that the device has a management interface that ANM can access. Also, you need the IP address and credentials for the device's management interface in order to import it.
- If the ACE module is new and retains its factory settings, you can configure basic management during the import process by using the Bare Blade option.

Procedure

Step 1 Choose **Config > Guided Setup > Import Devices**.

The Import Devices window appears, which includes the All Devices table.

Step 2 At the top of the All Devices table, click **Add** (+) to import a new device.

The New Device window appears.

Step 3 Enter the information for the specific device and complete the import devices procedure as described in "Importing Network Devices into ANM" section on page 4-9.

Note To manage modules inside a Catalyst 6500 series switch, you must first import the Catalyst into the All Devices table.

To import modules from a Catalyst that is already imported, choose the Catalyst switch from the All Devices table and click **Modules** below the All Devices table.

Note The time required to import depends on the size of the existing configuration on each device. The process can range from a few minutes to 30 minutes or more for a very large configuration.

Step 4 After you finish importing the ACE devices (module or appliance) into ANM, continue to the ACE Hardware Setup task to guide you through the basic device setup and network configuration. See the "Using ACE Hardware Setup" section on page 3-4.

Related Topics

- Information About Importing Devices, page 4-3
- Preparing Devices for Import, page 4-4
- Importing Network Devices into ANM, page 4-9
- Discovering Large Numbers of Devices Using IP Discovery, page 4-25
- Using ACE Hardware Setup, page 3-4

Using ACE Hardware Setup

You can use the ACE Hardware Setup task to configure ACE devices that are new to the network by establishing network connectivity in either standalone or high-availability (HA) deployments.

Before You Begin

Before you can set up the ACE hardware using ANM, you must use the Import Devices task to import the ACE into ANM if you have not already. See the "Using Import Devices" section on page 3-3.

Assumptions

- You can extend the functionality of the ACE by installing licenses. If you plan to extend the ACE functionality, ensure that you have received the proper software license key for the ACE, that ACE licenses are available on a remote server for importing to the ACE, or you have received the software license key and have copied the license file to the disk0: file system on the ACE using the **copy** *path/\filename1* **disk0:** CLI command.

Note See either the *Cisco Application Control Engine Module Administration Guide* or *Cisco 4700 Series Application Control Engine Appliance Administration Guide* for details on the **copy** *path/\filename1* **disk0:** CLI command.

- You must be in the Admin virtual context on an ACE device (ACE module or ACE appliance) to configure ACE devices that are new to the network.
- When importing an ACE HA pair into ANM, you should follow one of the following configuration requirements so that ANM can uniquely identify the ACE HA pair:
  - Use a unique combination of FT interface VLAN and FT IP address/peer IP address for every ACE HA pair imported into ANM. For HA, it is critical that the combination of FT interface VLAN and IP address/peer IP address is always unique across every pair of ACE peer devices.

– Define a peer IP address in the management interface using the management IP address of the peer ACE (module or appliance). The management IP address and management peer IP address used for this definition should be the management IP address used to import both ACE devices into ANM.

Note For more information about the use of HA pairs imported into ANM, see "ANM Requirements for ACE High Availability" section on page 4-7.

- When you are configuring the ACE, changes to the physical interfaces (including Gigabit Ethernet ports or port channels) can result in a loss of connectivity between ANM and the ACE. Use caution when following the ACE Hardware Setup task if you are modifying the interface that management traffic is traversing.

Procedure

Step 1 Choose **Config > Guided Setup > ACE Hardware Setup**.

The ACE Hardware Setup window appears, which includes the ACE Device and Configuration Type drop-down lists.

Step 2 From the ACE Device drop-down list, choose an ACE device (module or appliance).

Step 3 From the Configuration Type drop-down list, choose whether to set up the ACE as a standalone device or as a member of a high-availability (HA) ACE pair:

- Standalone—The ACE is not to be used in an HA configuration.
- HA Secondary—The ACE is to be the secondary peer in an HA configuration.
- HA Primary—The ACE is to be the primary peer in an HA configuration.

Note Ensure that you complete the ACE hardware setup task for the secondary device *before* you set up the primary device.

Step 4 Click **Start Setup**.

The License window appears (Config > Guided Setup > ACE Hardware Setup > Licenses). Cisco offers licenses for ACE modules and appliances that allows you to increase the number of default contexts, bandwidth, and SSL TPS (transactions per second). For more information, see either the *Cisco Application Control Engine Module Administration Guide* or to the *Cisco 4700 Series Application Control Engine Appliance Administration Guide* on cisco.com.

If you need to install licenses at this point, go to Step 5.

If you do not need to install licenses at this point, go to Step 6.

Step 5 Install one or more ACE licenses (see the "Managing ACE Licenses" section on page 5-34).

Note For an ACE primary and secondary HA pair, because each ACE license is only valid on a single hardware device, licenses are not synchronized between HA peer devices. You must install an appropriate version of each license independently on both the primary and secondary ACE devices.

Step 6 Click **SNMP v2c Read-Only Community String** under ACE Hardware Setup (Config > Guided Setup > ACE Hardware Setup > SNMP v2c Read-Only Community String).

The SNMP v2c Read-Only Community String window appears.

Perform the following actions to configure an SNMP community string (a requirement for an ACE to be monitored by ANM):

a. Click **Add** (+) at the top of the SNMP v2c Read-Only Community String table to create an SNMP community string. The New SNMP v2c Community window appears.

Note For ANM to monitor an ACE, you must configure an SNMPv2c community string in the Admin virtual context.

b. In the Read-Only Community field, enter the SNMP read-only community string name. Valid entries are unquoted text strings with no spaces and a maximum of 32 characters.

Additional SNMP configuration selections are available under Config > Devices > context > System > SNMP. See the "Configuring SNMP for Virtual Contexts" section on page 5-25.

Step 7 If you are configuring an ACE appliance, to group physical ports together on the ACE appliance to form a logical Layer 2 interface called the port-channel (sometimes known as EtherChannels), click **Port Channel Interfaces** under ACE Hardware Setup.

The Port Channel Interfaces window appears (Config > Guided Setup > ACE Hardware Setup > Port Channel Interfaces).

Note You must configure port channels on both the ACE appliance and the switch that the ACE is connected to.

Perform the following actions to configure a port channel interface:

a. If you want to poll the devices and display the current values, click **Poll Now**, and then **OK** when prompted if you want to poll the devices for data now.

b. At the top of the Port Channel Interfaces table, click **Add** (+) to add a port channel interface, or choose an existing port channel interface and click **Edit** to modify it. The New Port Channel Interface window appears.

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

c. Enter the port channel interface attributes as described in the "Configuring Port-Channel Interfaces for the ACE Appliance" section on page 11-24.

d. Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.

e. To display statistics and status information for a 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.

Step 8 If you are configuring an ACE appliance, to configure one or more of the Gigabit Ethernet ports on the appliance, click **GigabitEthernet Interfaces** under ACE Hardware Setup. The GigabitEthernet Interfaces window appears (Config > Guided Setup > ACE Hardware Setup > GigabitEthernet Interfaces).

a. If you want to poll the devices and display the current values, click **Poll Now**, and then **OK** when prompted if you want to poll the devices for data now.

b. Choose an existing Gigabit Ethernet interface and click **Edit** to modify it.

c. Enter the Gigabit Ethernet physical interface attributes as described in the "Configuring Gigabit Ethernet Interfaces on the ACE Appliance" section on page 11-21.

d. Click **Deploy Now** when completed to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.

e. Repeat Steps a through c for each Gigabit Ethernet interface that you want to configure.

f. To display statistics and status information for a particular Gigabit Ethernet interface, choose the interface from the GigabitEthernet Interfaces table, then 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.

Step 9 If the ACE is a member of an HA ACE pair, click **VLAN Interfaces** under ACE Hardware Setup.

The VLAN Interfaces window appears (Config > Guided Setup > ACE Hardware Setup > VLAN Interfaces).

Note To prevent loss of management connectivity during an HA configuration, you must configure the IP addresses of the management VLAN interface correctly for your HA setup. During this procedure, choose the management VLAN interface (and click the **Edit** button) and make sure its IP address, alias IP address, and peer IP address are all set correctly. You can repeat this process for any VLAN interfaces that you want. If the management VLAN is properly configured before establishing HA, you will be able to return later to reconfigure other VLANs.

a. If you want to poll the devices and display the current values, click **Poll Now**, and then **OK** when prompted if you want to poll the devices for data now.

b. 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.

c. Enter the VLAN interface attributes as described in the "Configuring VLAN Interfaces" section on page 11-5. Click **More Settings** to access the additional VLAN interface attributes. By default, ANM hides the default VLAN interface attributes and the VLAN interface attributes which are not commonly used.

d. Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.

e. 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.

Step 10 If the ACE is the primary peer in a high availability (HA) configuration, click **HA Peering** under ACE Hardware Setup (Config > Guided Setup > ACE Hardware Setup > HA Peering).

a. Click **Edit** below the HA Management section to configure the primary ACE and the secondary ACE as described in the "Configuring ACE High Availability Peers" section on page 12-14. There are two columns, one for the selected ACE and another for a peer ACE.

You can specify the following information:

- Identify the two members of a HA pair.
- Assign IP addresses to the peer ACEs.
- Assign an HA VLAN to HA peers and bind a physical Gigabit Ethernet interface to the FT VLAN.
- Configure the heartbeat frequency and count on the peer ACEs in a fault-tolerant VLAN.

When completed, click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.

Note For ACE modules, the HA VLAN specified for ACE HA Groups must also be set up on the Catalyst 6500 series switch using the **svclc** command. See the "Configuring VLANs Using Cisco IOS Software (ACE Module)" section on page 11-3 for details.

b. Click **Add** below the ACE HA group table to add a new high availability group. Enter the information in the configurable fields as described in the "Configuring ACE High Availability Peers" section on page 12-14. When completed, click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.

The HA State field displays FT VLAN Compatible once HA setup has been successfully completed.

Note To display statistics and status information for a particular HA group, choose the group from the ACE HA Groups table and click **Details**. The **show ft group** *group_id* **detail** CLI command output appears. See the "Displaying High Availability Group Statistics and Status Information" section on page 12-22 for details.

Step 11 Once the HA State field in the ACE HA Groups table shows a successful state, the ACE is ready for further configuration as follows:

- To set up additional virtual contexts, continue to the Virtual Context Setup task to create and connect an ACE virtual context. See the "Using Virtual Context Setup" section on page 3-9.
- To set up an application in an existing virtual context, continue to the Application Setup task to set up load-balancing for an application from an ACE to a group of back-end servers. See the "Using Application Setup" section on page 3-11.

Related Topics

- Using Import Devices, page 3-3
- Configuring Devices, page 4-32
- Configuring ACE Module and Appliance Role-Based Access Controls, page 4-51
- Managing Devices, page 4-64

Using Virtual Context Setup

You can use the Virtual Context Setup task to create and connect an ACE virtual context. Virtual contexts use virtualization to partition your ACE appliance or module into multiple virtual devices, or contexts. Each context contains its own set of policies, interfaces, resources, and administrators.

Before You Begin

You must be in the Admin context on the ACE to create a new user context.

Procedure

Step 1 Choose **Config > Guided Setup > Virtual Context Setup**.

The Virtual Context Setup window appears.

Step 2 From the ACE Device drop-down list, choose an ACE.

Step 3 Click **Start Setup**.

The Resource Classes window appears (Config > Guided Setup > Virtual Context Setup > Resource Classes).

Perform the following tasks to create or modify a resource class:

a. If you want to create a resource class, click **Add (+)**. The New Resource Class configuration window appears. Enter the resource information as described in the "Configuring Global Resource Classes" section on page 5-44.

b. If you want to modify an existing resource, choose the resource class that you want to modify, then click **Edit**. The Edit Resource Class configuration window appears. Enter the resource information as described in the "Modifying Global Resource Classes" section on page 5-48.

c. Click **OK** to save your entries and to return to the Resource Classes table.

Make note of the resource class that you want to use because you will need it in Step 5.

Step 4 Click **Virtual Context Management** under Virtual Context Setup.

The Virtual Context window appears (Config > Guided Setup > Virtual Context Setup > Virtual Context Management).

Perform the following actions to create or modify a virtual context:

a. If you want to create a virtual context, click **Add (+)**. The New Virtual Context window appears. Configure the virtual context as described in the "Configuring Virtual Contexts" section on page 5-7.

b. If you want to modify an existing virtual context, choose the virtual context that you want to modify and click **Edit**. The Edit Resource Class configuration window appears. Enter the resource information as described in the "Modifying Global Resource Classes" section on page 5-48.

Step 5 To create or modify the attributes of a virtual context, configure the virtual context as described in the "Configuring Virtual Contexts" section on page 5-7.

When completed, click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files. Follow these guidelines when creating or modifying the virtual context:

- To connect the virtual context to the available VLANs, specify one or more VLANs in the Allocated VLANs field. You can specify multiple VLAN values and ranges (for example, "10, 14, 70-79").
- For virtual contexts configured for an ACE, do the following:

  - For an ACE appliance, you must set up all VLANs used in this step as trunk or access VLANs on the port channel or Gigabit Ethernet interfaces. If you did not set up these VLANs during the ACE Hardware Setup task, you can return to the ACE Hardware Setup window to configure the required VLANs. See the "Using ACE Hardware Setup" section on page 3-4.
  - For an ACE module, you must set up all VLANs used in this step as trunk or access VLANs on the Catalyst 6500 series switch using the **svclc** command. See the "Configuring VLANs Using Cisco IOS Software (ACE Module)" section on page 11-3 for details.

- When specifying the resource class for the virtual context, choose the resource class that you created or specified in Step 3.

  Note If you are unsure of the resource class to use for this virtual context, choose **default**. You can change the resource class setting at a later time.

- If HA has been correctly configured for this ACE device, the High Availability checkbox will be checked. If the checkbox is unchecked, check it to instruct ANM to automatically configure synchronization for this virtual context.

  Note The High Availability checkbox is available only if HA Peering has previously been completed for the ACE hardware.

- If you want to set up a separate management VLAN interface for the virtual context, under Management Settings, configure the management interface for this virtual context and create an admin user. Each context also has its own management VLAN that you can access using the ANM GUI. In this case, you would assign an independent VLAN and IP address for management traffic to access the virtual context.

Step 6 To edit the load-balancing configuration for a virtual context, continue to the Application Setup task. See the "Using Application Setup" section on page 3-11.

Related Topics

- Using Import Devices, page 3-3
- Using ACE Hardware Setup, page 3-4
- Information About Virtual Contexts, page 5-2
- Using Resource Classes, page 5-41
- Creating Virtual Contexts, page 5-2
- Configuring Virtual Contexts, page 5-7
- Configuring VLANs Using Cisco IOS Software (ACE Module), page 11-3
- Using Application Setup, page 3-11

Using Application Setup

This section includes the following topics on application setup:

ACE Network Topology Overview

With respect to ACE configuration, the network topology describes where—which VLAN or subnet—client traffic comes into the ACE and where this traffic is sent to real servers. Network configuration for ACE load balancing depends on the surrounding topology. By specifying to ANM the topology that is appropriate for your networking application, ANM can present more relevant options and guidance.

The network topology is often determined solely by your existing network; however, the goals for your ACE deployment can also play a role. For example, when ACE acts as a router between clients and servers, it provides a level of protection by effectively hiding the servers from the clients. On the other hand, for a routed topology to work, each of those servers must be configured to route back through the ACE, which can be a significant change to the network routing.

The ACE is also capable of bridging the client and server VLANs, which does not affect server routing. However, it does require the network to have VLANs set up appropriately.

If you are not sure what topology to use, or do not want to make topology decisions immediately, use the "one-armed" topology. The one-armed topology does not typically require any changes to an existing network and can be set up with minimal knowledge of the network. You can then expand your ACE network topology to routed mode or bridged mode to better suit your networking requirements.

Figure 3-1illustrates the one-armed network topology.

Figure 3-1 Example of a One-Armed Network Topology

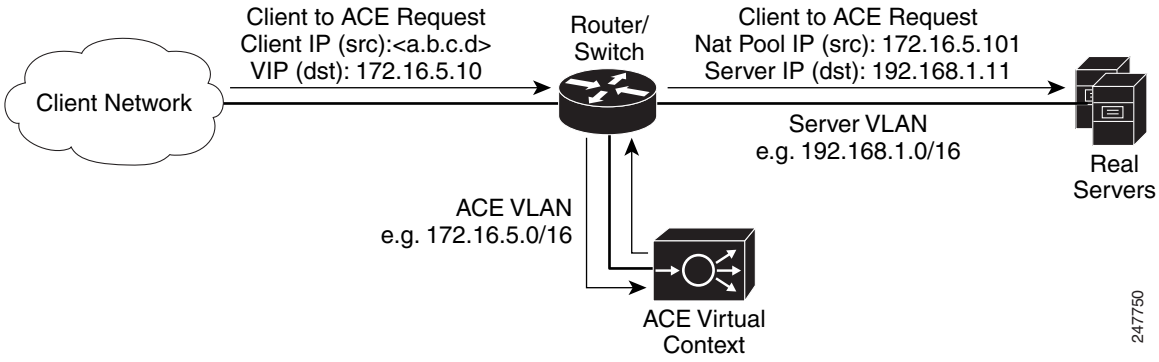


Figure 3-2illustrates the routed mode network topology.

Figure 3-2 Example of a Routed Mode Network Topology

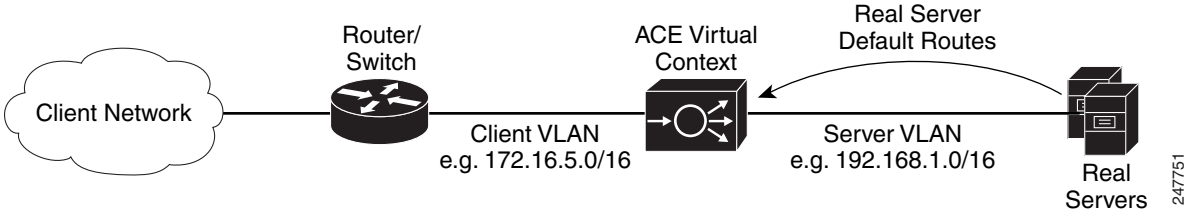
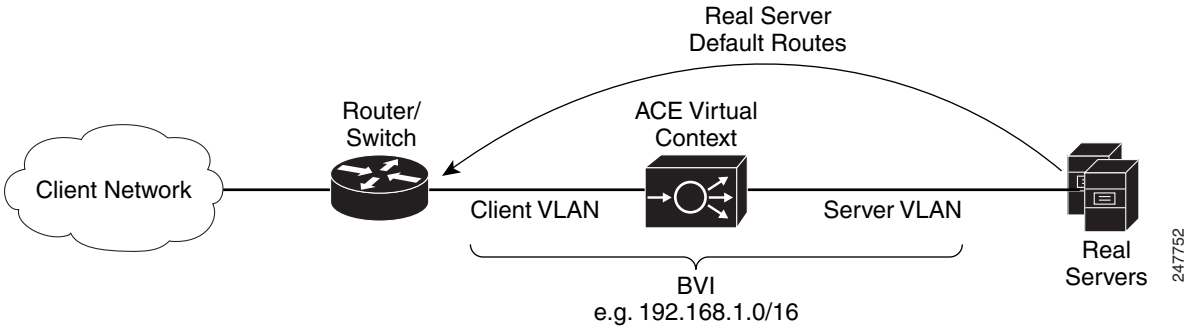


Figure 3-3illustrates the bridged mode network topology.

Figure 3-3 Example of a Bridged Mode Network Topology



Using Application Setup

You use the Application Setup task to set up load balancing for an application.

Procedure

Step 1 Choose **Config > Guided Setup > Application Setup**.

The Application Setup window appears.

Step 2 From the Select Virtual Context drop-down list, choose an existing ACE virtual context.

Step 3 If your ACE is to use HTTPS when communicating with either the client or with real servers, in the Use HTTPS (SSL) field, choose **Yes** to specify that the ACE should be set up for secure (SSL) Hypertext Transfer Protocol (HTTP).

Step 4 Choose the network topology that reflects the relationship of the selected ACE virtual context to the real servers in the network.

Topology choices include one-armed, routed, or bridged. See the "ACE Network Topology Overview" section on page 3-11 for background details on networking topology.

Step 5 Click **Start Setup**.

Step 6 If you selected either the one-armed or routed topology, the VLAN Interfaces window appears (Config > Guided Setup > Application Setup > VLAN Interfaces).

To communicate with the client and real servers, a VLAN interface must be specified for client and server traffic to be sent and received.

Perform the following actions to configure a VLAN interface:

a. If you want to poll the devices and display the current values, click **Poll Now**, and then click **OK** when prompted to poll the devices for data.

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

c. Enter the VLAN interface attributes as described in the "Configuring VLAN Interfaces" section on page 11-5. Click **More Settings** to access the additional VLAN interface attributes. By default, ANM hides the default VLAN interface attributes and the VLAN interface attributes which are not commonly used.

Note After you define the VLAN, write down the VLAN number. You will need this VLAN number in the ACL and virtual server steps (Steps 9 and 11) of this procedure.

d. Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.

e. 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.

Step 7 If you selected the bridged topology, the BVI Interfaces window appears (Config > Guided Setup > Application Setup > BVI Interfaces).

Perform the following actions to configure a BVI interface:

a. If you want to poll the devices and display the current values, click **Poll Now**, and then **OK** when prompted if you want to poll the devices for data now.

b. Click **Add** to add a new BVI interface, or choose an existing BVI interface, then click **Edit** to modify it.

c. Enter the BVI interface attributes as described in the "Configuring Virtual Context BVI Interfaces" section on page 11-13.

Note After you define the BVI, write down the client-side VLAN number. You will need this BVI number in the ACL and virtual server steps (Steps 9 and 11) of this procedure.

d. Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.

e. To display statistics and status information for a BVI interface, choose the BVI interface from the BVI Interface table, then click **Details**. The **show interface bvi** CLI command output appears. See the "Displaying VLAN Interface Statistics and Status Information" section on page 11-12 for details.

Step 8 If you selected the one-armed topology, click **NAT Pools** under Application Setup.

The NAT Pools window appears (Config > Guided Setup > Application Setup > NAT Pools). To set up a one-armed topology, you need a NAT pool to provide the set of IP addresses that ACE can use as source addresses when sending requests to the real servers.

Note You must configure the NAT pool on the same VLAN interface that you configured in Step 6.

Perform the following actions to create or modify a NAT pool for a VLAN:

a. Click **Add** to add a new NAT pool entry, or choose an existing NAT pool entry and click **Edit** to modify it. The NAT Pool configuration window appears.

b. Configure the NAT pool attributes as described in the "Configuring VLAN Interface NAT Pools" section on page 11-16.

Note After you define the NAT pool, write down the NAT pool ID. You will specify the NAT pool ID in the virtual server step (Step 11) of this procedure.

c. Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.

Step 9 Click **ACLs** under Application Setup.

The ACLs window appears (Config > Guided Setup > Application Setup > ACLs). An ACL applies to one or more VLAN interfaces. Each ACL consists of a list of entries, each of which defines a source, a destination, and whether to permit or deny traffic between those locations.

Perform the following actions to create or modify an ACL:

a. Click **Add** to add a new ACL entry, or choose an existing ACL entry and click **Edit** to modify it. The Access List configuration window appears.

b. Add or edit the required fields as described in the "Configuring Security with ACLs" section on page 5-74.

c. Click **Deploy** to save this configuration.

d. To display statistics and status information for an ACL, choose an ACL from the ACLs table, then click **Details**. The **show access-list** *access-list* **detail** CLI command output appears. See the "Displaying ACL Information and Statistics" section on page 5-83 for details.

Step 10 Click **SSL Proxy** under Application Setup.

This selection appears only if you specified in Step 3 that the ACE is to use HTTPS when communicating with either the client or with real servers.

The SSL Proxy window appears (Config > Guided Setup > Application Setup > SSL Proxy).

Note To terminate or initiate HTTPS connections with ACE, the virtual context must have at least one SSL proxy service. An SSL proxy contains the certificate and key information needed to terminate HTTPS connections from the client or initiate them to the servers.

Perform the following actions to create or modify an SSL proxy service:

a. To create an SSL proxy service, click **SSL Proxy Setup**.

Note To edit an existing SSL proxy service, choose it from the SSL Proxy table, and click **Edit** to modify the SSL proxy service. The SSL Proxy Service configuration window appears. Edit the required fields as described in the "Configuring SSL Proxy Service" section on page 10-27.

b. Add required fields as described in the "Configuring SSL Proxy Service" section on page 10-27.

c. Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.

Step 11 Click **Virtual Server** under Application Setup.

The Virtual Servers window appears (Config > Guided Setup > Application Setup > Virtual Server). The virtual server defines the load-balancing configuration for an application.

Perform the following actions to create or modify a virtual server:

a. If you want to poll the devices and display the current values, click **Poll Now**, and then **OK** when prompted if you want to poll the devices for data now.

b. Click **Add** to add a new virtual server, or choose an existing virtual server, and click **Edit** to modify it. The Virtual Server configuration window appears with a number of configuration subsets. The subsets that you see depend on whether you use the Basic View or the Advanced View and entries you make in the Properties subset. Change views by using the View object selector at the top of the configuration pane.

c. Add or edit required fields as described in the "Virtual Server Configuration Procedure" section on page 6-7. Table 6-1 identifies and describes virtual server configuration subsets with links to related topics for configuration information.

Virtual servers have many configuration options. At a minimum, you need to configure the following attributes:

– Set the VIP, port number (TCP or UDP), and application protocol for your application.

Note If the ACE is to terminate the client HTTPS connections, choose **HTTPS** as the Application Protocol.

– (One-Armed Topology) For VLAN, choose the VLAN from Step 6.

– (Routed Topology) For VLAN, choose the client-side VLAN from Step 6.

– (Bridged Topology) For VLAN, choose the client-side VLAN from Step 6.

– If the ACE is to terminate client HTTPS connections, then under the SSL Termination header, specify the SSL proxy defined in Step 10.

– Under the Default L7 Loadbalancing Action, set Primary Action to **Loadbalance**.

– Create a server farm that contains one or more real servers for this application (see Table 6-13 in the "Configuring Virtual Server Layer 7 Load Balancing" section for details on setting server farm attributes).

– If the ACE is to initiate HTTPS connections to the real servers, choose the desired SSL proxy for initiation to this application from the menu next to SSL Initiation.

– (One-Armed Topology) Under NAT, enter the NAT pool ID from Step 8.

After you set up a base virtual server, you can test it to validate your configuration and isolate any issues in your networking application. You can then add these more advanced load balancing options to your networking application:

– Additional real servers to a server farm. See Table 6-13 in the "Configuring Virtual Server Layer 7 Load Balancing" section for details.

– Health monitoring probes and attributes for the specific probe type. See Table 6-14 in the "Configuring Virtual Server Layer 7 Load Balancing" section for details.

- Stickiness, where client requests for content are to be handled by a sticky group when match conditions are met. See Table 6-15 in the "Configuring Virtual Server Layer 7 Load Balancing" section for details.
- Application protocol inspection, where the ACE allows the virtual server to verify protocol behavior and identify unwanted or malicious traffic passing through the ACE. See the "Configuring Virtual Server Protocol Inspection" section for details.

d. Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.

e. To display statistics and status information for an existing virtual server, choose a virtual server from the Virtual Servers table, then click **Details**. The **show service-policy global detail** CLI command output appears. See the "Displaying Virtual Server Statistics and Status Information" section on page 6-64 for details.

Related Topics

- Using Import Devices, page 3-3
- Using ACE Hardware Setup, page 3-4
- Using Virtual Context Setup, page 3-9
- Configuring VLAN Interfaces, page 11-5
- Configuring Virtual Context BVI Interfaces, page 11-13
- Configuring Virtual Context Static Routes, page 11-18
- Configuring Virtual Context BVI Interfaces, page 11-13
- Configuring Security with ACLs, page 5-74
- SSL Setup Sequence, page 10-4