CHAPTER 4

Adding and Managing Devices

Date: 1/10/13

This chapter describes how to add and manage Cisco Application Networking Manager (ANM) devices. You can add the following Cisco devices to ANM:

- Application Control Engine (ACE) module or appliance
- Global Site Selector (GSS)
- Content Services Switch (CSS)
- Catalyst 6500 Virtual Switching System (VSS) 1440
- Catalyst 6500 series switch
- Cisco 7600 series router
- Cisco Content Switching Module (CSM)
- Cisco Content Switching Module with SSL (CSM-S)

Note The terms *add* and *import* are interchangeable in this document.

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 Device Management, page 4-2
- Information About Importing Devices, page 4-3
- Preparing Devices for Import, page 4-3
- Adding Network Devices into ANM, page 4-9
- Discovering Large Numbers of Devices Using IP Discovery, page 4-21
- Configuring Devices, page 4-27

- Configuring ACE Module and Appliance Role-Based Access Controls, page 4-45
- Managing Devices, page 4-58
- Synchronizing Module Configurations, page 4-59
- Synchronizing Device Configurations, page 4-58
- Restarting Device Polling, page 4-66
- Configuring User-Defined Groups, page 4-60

Information About Device Management

ANM includes many device management features. You can add devices and then configure them for use in your network. In addition to configuring ports, VLANs, and routes, you can modify device configurations, and manage them.

Table 4-1 identifies common management categories and related topics.

Table 4-1 Device Management Options

Device Management Activities	Related Topics
Adding and importing devices	• Information About Importing Devices, page 4-3 • Preparing Devices for Import, page 4-3 • Enabling SSH or Telnet Access on Catalyst 6500 Series Switches and Cisco 7600 Series Routers, page 4-4 • Adding Network Devices into ANM, page 4-9 • Adding ACE Modules to ANM, page 4-14 • Instructing ANM to Recognize an ACE Module Software Upgrade, page 4-16 • Importing CSM Devices, page 4-17 • Importing GSS Devices, page 4-18 • Discovering Large Numbers of Devices Using IP Discovery, page 4-21
Configuring device attributes	• Configuring Devices, page 4-27 • Configuring CSM Primary Attributes, page 4-27 • Configuring CSS Primary Attributes, page 4-28 • Configuring GSS Primary Attributes, page 4-29 • Configuring Catalyst 6500 Series Chassis and Cisco 7600 Series Router Primary Attributes, page 4-31 • Configuring Catalyst 6500 Series Chassis, Catalyst 6500 Virtual Switching System 1440 Devices, and Cisco 7600 Series Routers Static Routes, page 4-32 • Displaying Chassis Interfaces and Configuring High-Level Interface Attributes, page 4-34 • Managing Catalyst 6500 Series Chassis or Cisco 7600 Series Router VLANs, page 4-40 • Creating VLAN Groups, page 4-44

Table 4-1 Device Management Options (continued)

Device Management Activities	Related Topics
Configuring device role-based access control (RBAC)	• Configuring Device RBAC Users, page 4-45 • Configuring Device RBAC Roles, page 4-49 • Configuring Device RBAC Domains, page 4-53
Managing devices	• Synchronizing Device Configurations, page 4-58 • Configuring User-Defined Groups, page 4-60 • Updating Device Passwords, page 4-64 • Changing ACE Module Passwords, page 4-65 • Restarting Device Polling, page 4-66 • Displaying All Devices, page 4-67 • Displaying Modules by Chassis, page 4-68 • Removing Modules from the ANM Database, page 4-69

Information About Importing Devices

The quickest and easiest way to add devices to ANM is to import them individually using the Add function available at Config > Devices. If you already know the device IP address, you can use this procedure to add your devices to ANM.

Before you begin importing, you need to set up your network devices so that ANM can communicate and monitor them.

In the sections that follow, you will perform the following two steps to prepare and import devices:

1. Enable SSH access (see the "Preparing Devices for Import" section on page 4-3).
2. Import devices (see the "Adding Network Devices into ANM" section on page 4-9).

To add large numbers of devices, you can use IP Discovery before you import your devices. This process is not as efficient as using the Add function. IP Discovery shows where devices are but does not add the devices to ANM. We recommend that you use the Config > Devices > Add function. For details on IP Discovery, see the "Discovering Large Numbers of Devices Using IP Discovery" section on page 4-21.

Note Before importing a device, the ANM server pings the IP address of the device. If you have a firewall between the ANM server and the device that you want to import, your network administrator needs to modify the firewall to allow the ping traffic to reach the device or ACE.

Preparing Devices for Import

This section describes how to set up your devices to allow ANM to communicate with them and also describes the requirements for adding ACE devices that are high availability peers.

ANM uses the following protocols for communication:

- For communication to an ACE module or appliance:
  - XML over HTTPS

  - SSHv2 (read and write)
  - SNMP V2C (read-only)
  - Syslog over User Datagram Protocol (UDP) (inbound notifications only)
- For communication to the Catalyst 6500 Virtual Switching System (VSS) 1440:
  - SSHv2 and Telnet (read and write)
  - SNMP V2C (read-only)
  - Syslog over UDP (inbound notifications only)
- For communication to a Catalyst 6500 series switch, Cisco 7600 series router, CSM, or CSM-S:
  - SSHv2 and Telnet (read and write)
  - SNMP V2C (read-only)
  - Syslog over UDP (inbound notifications only)
- For communication to the CSS:
  - Telnet (read and write)
  - SNMP V2C (read-only)
  - Syslog over UDP (inbound notifications only)
- For communication to the GSS:
  - SSHv2
  - Remote Method Invocation (RMI) over SSL

Note Before you import a GSS device into ANM, you need to set the GSS communication on the GSS Ethernet interface that will be used to import the GSS into ANM. See the *Cisco Global Site Selector Command Reference* on Cisco.com for instructions on using the **gss-communications** command.

This section includes the following topics:

- Enabling SSH or Telnet Access on Catalyst 6500 Series Switches and Cisco 7600 Series Routers, page 4-4
- Enabling SSH Access and the HTTPS Interface on the ACE Module and Appliance, page 4-5
- Enabling SNMP Polling from ANM, page 4-6
- ANM Requirements for ACE High Availability, page 4-7

Enabling SSH or Telnet Access on Catalyst 6500 Series Switches and Cisco 7600 Series Routers

You can choose to use Telnet or SSH to import a Catalyst 6500 series switch or Cisco 7600 series router in ANM. Telnet is enabled by default on the Catalyst 6500 series chassis. If you have disabled Telnet on the device, you need to enable it to perform the initial setup and import of an ACE module. If you plan to directly import an ACE module into ANM, Telnet is not mandatory on a Catalyst 6500 series switch.

Note If you choose Telnet, the Use Telnet checkbox will be checked in the Primary Attributes window (see the "Configuring Catalyst 6500 Series Chassis and Cisco 7600 Series Router Primary Attributes" section on page 4-31).

If you use SSH to communicate with the device, you must do the following:

- SSHv2 must be enabled on the chassis, as well as the ACE, in order for ANM to add device information about the chassis.
- Ensure that the chassis has a K9 (Triple Data Encryption Standard [3DES]) software image in order to enable the SSH server. The ANM requires SSHv2 to be enabled on the chassis.

To enable SSH or Telnet access on Catalyst 6500 series switches or Cisco 7600 series routers, use the following commands:

	Command	Purpose
Step 1	`ip ssh version 2`	Enables SSHv2.
Step 2	`ip domain-name abc.com`	
Step 3	`crypto key generate rsa general-keys modulus 1024`	Generates the key.
Step 4	`username <username> password <password>`	Enters the username and password.
Step 5	`line vty 0 4`	
Step 6	`session-timeout 60`	
Step 7	`login local`	This is an example only. This commands works for Cisco IOS 12.2.18SXF(10), but not for 12.2.18SXF(8).
Step 8	`transport input telnet ssh`	Allows SSH and Telnet to the chassis.
Step 9	`transport output telnet ssh`	Allows SSH and Telnet from the chassis to the ACE module.

Enabling SSH Access and the HTTPS Interface on the ACE Module and Appliance

You can enable SSH access and the HTTPS interface on the ACE modules and appliances. ANM uses SSH and XML over HTTPS to communicate with the ACE devices. You need to enable both SSH access and HTTPS as explained in this section. These settings can be enabled during device import as described in the "Adding Network Devices into ANM" section on page 4-9 or in the CLI.

Note If the ACE module or appliance is new and still has its factory settings, you do not need to perform the procedure in this section because SSH is enabled by default.

Note Ensure that the management policy applied on the management interface permits SSH.

To enable SSH access and the HTTPS interface on an ACE module or appliance, enter the following commands in config mode in the Admin context:

	Command	Purpose
Step 1	`ssh key rsa 1024 force`	Configures SSH access on the ACE.
Step 2	`access-list acl line 10 extended permit ip any any`	

Step 3	`class-map type management match-any ANM_management`
	
	`2 match protocol ssh any`
	`3 match protocol telnet any`
	`4 match protocol https any`
	`5 match protocol snmp any`
	`6 match protocol icmp any`
	`7 match protocol xml-https`
		Configures discovery for ANM.
		
		The following comments apply to the line number specified before the command text in the left column:
		• Line 2 classifies the SSH traffic.
		• Line 4 is needed by ANM for making configuration changes on the ACE.
		• Line 5 is needed by ANM for periodic statistics.
		• Line 6 is not mandatory but useful for network and route validation.
		• Line 7 is needed only for ACE 4710 devices.

Step 4	`policy-map type management first-match ANM_management`
	`class ANM_management`
	`permit`
		Allows protocols matched in the management class map.

Step 5	`interface vlan 30`
	`ip address 192.168.65.131 255.255.255.0`
	`access-group input acl`
	`service-policy input ANM_management`
	`no shutdown`
		Configures a management interface with the ACL and specifies the management service policy. This configuration is not recommended for a client or server interface.

Step 6	`username admin password 5 $1$faXJEFBj$TJR1Nx7sLPTi5BZ97v08c/ role Admin domain default-domain`	Defined by the administrator.
Step 7	`ip route 0.0.0.0 0.0.0.0 192.168.0.1`	Specifies the default route (or appropriate route) for traffic to reach ANM using the management interface if ANM is not on the same subnet.

For more information about configuring SSH access on the ACE, see either the *Cisco Application Control Engine Module Administration Guide* or the *Cisco 4700 Series Appliance Administration Guide* on Cisco.com.

Enabling SNMP Polling from ANM

You can enable SNMP polling from ANM.

Note To send SNMP traps to ANM, configure the SNMP trap host to the ANM server so that it can receive traps from ANM.

For the ACE, in order for ANM to successfully perform SNMP polling, you must configure the ACE Admin context with a management IP with a suitable management policy that permits SNMP traffic. All other contexts can be polled using this Admin context management IP.

For each device type (ACE, CSS, CSM, or CSM-S), see the corresponding configuration guide to configure the device to permit SNMP traffic.

ANM Requirements for ACE High Availability

ANM automatically identifies ACE high availability (HA) peers if both peers are imported into ANM. For ANM to identify two ACE devices (ACE modules or ACE appliances) as high availability peers, ANM looks for two ACE devices with the same fault-tolerant (FT) interface VLAN configuration and whose peer IP addresses are reversed.

For example, ANM would consider Peer 1 with the following configuration:

```
ft interface vlan 4000
  ip address 10.10.10.1 255.255.255.0
  peer ip address 10.10.10.4 255.255.255.0
```

and Peer 2 with the following configuration:

```
ft interface vlan 4000
  ip address 10.10.10.4 255.255.255.0
  peer ip address 10.10.10.1 255.255.255.0
```

as HA peers because they both use FT interface VLAN 4000 and their IP and peer IP addresses are reversed.

However, it is possible that multiple ACE devices imported into ANM have the same FT interface VLAN and IP address/peer IP address combinations. In this case, ANM is not able to identify the ACE HA pair correctly. To resolve this issue, ANM uses the following logic to determine that two ACE devices are an HA pair:

1. Two ACE devices could be identified as a HA pair if their FT interface VLAN IDs match and their FT interface IP and peer IP addresses are reversed.
2. If the Admin context management interface peer IP address is already defined, ANM will conclusively identify its HA peer if the other Admin context management interface reversely matches the management IP and peer IP addresses.
3. If both ACE Admin context management interface peer IP addresses are not defined, and their FT interface configuration combination is unique across all ACE devices, ANM will then identify them as an HA pair.
4. An ACE HA peer is identified as Inconclusive if there is a non unique FT interface configuration combination across all ACE devices and its Admin context management interface peer IP is not defined.

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.

An example is as follows:

- ACE1 is imported into ANM with management IP 10.10.10.10.
- ACE2 is imported into ANM with management IP 10.10.10.12.

In this case, you would perform the following actions for both ACE1 and ACE2:

- Update the management interface on ACE1 with IP address 10.10.10.10. to have 10.10.10.12 as the peer IP address.
- Update the management interface on ACE2 with IP address 10.10.10.12 to have 10.10.10.10 as the peer IP address.

An ACE module or appliance may have many other management interfaces defined, but ANM is particularly interested only in the management interface whose IP address is used for importing into ANM.

When ANM is unable to determine a unique ACE HA peer pair, it displays an Inconclusive state in the ACE HA State column of the All Virtual Contexts table (Config > Devices > Virtual Context Management) or the Virtual Contexts listing page. The Inconclusive state indicates that ANM was able to determine that the given ACE was configured in HA; however, ANM was able to find more than one ACE module or ACE appliance that appeared to be a peer. In this case, ANM was unable to conclusively find a unique HA peer for the given ACE module or ACE appliance. You must then perform the actions outlined in this section to fix the ACE that is in this state.

More information will appear in the tooltip for the Inconclusive state to specify whether this state was reached because the FT interface VLAN and the IP address/peer IP address was not unique, or because the peer IP address on the management interface was not unique.

Based on the information provided to you in the tooltip for the Inconclusive state, you must update the ACE configuration as described in the configuration requirements outlined above. After you make these configuration changes, resynchronize the affected ACE devices in ANM to update the configuration and HA mapping. For more information about synchronizing virtual contexts, see the "Creating Virtual Contexts" procedure on page 5-2.

Adding Network Devices into ANM

ANM allows you to add the following devices individually to its database:

- ACE appliances
- ACE modules
- Catalyst 6500 series chassis
- Catalyst 6500 Virtual Switching System (VSS) 1440
- Cisco 7600 series routers
- Cisco Content Services Switch (CSS) devices
- Cisco Content Switching Module (CSM) devices
- Cisco Global Site Selector (GSS) devices

Note Before adding a device or ACE module, the ANM server pings the IP address of the device or ACE module. If you have a firewall between the ANM server and the device you want to import, your network administrator needs to modify the firewall to allow the ping traffic to reach the device or ACE module.

Note In order to import your ACE devices successfully, ensure the following:

- The ACE module or CSM has booted successfully and is in the OK/Pass state (enter the **show module** Supervisor IOS CLI command to verify this action).
- The ACE 4710 or the CSS state is up and running. There is no command to validate whether these devices are up and running.

We recommend that you use the procedures in this section to add your devices to ANM because they are faster and more efficient than running IP Discovery.

This section includes the following topics:

- Adding Devices to ANM, page 4-9
- Adding ACE Modules to ANM, page 4-14 (adds an ACE module when the host chassis has already been added)
- Importing CSM Devices, page 4-17 (adds a CSM when the host chassis has already been added)
- Importing GSS Devices, page 4-18.

Adding Devices to ANM

This section shows how to add a supported device to ANM. This method adds the devices individually to the ANM database instead of or in addition to running discovery and importing them from the Discovery Jobs table.

Note When adding a module device, such as an ACE module or a CSM, you first add the host chassis device, such as a ACE Catalyst 6500 series chassis, and then you add the module. To import an ACE module or CSM when the host chassis has already been added, see either the "Adding ACE Modules to ANM" section on page 4-14 or the "Importing CSM Devices" section on page 4-17.

Note The time required to import devices depends on the number of appliances, chassis, modules, and contexts that you are importing. For example, an ACE appliance with 50 virtual contexts takes longer than an ACE appliance with 25 contexts. While ANM imports devices, you cannot perform other activities in the same session. You can, however, establish a new session with the ANM server and perform activities on other appliances, chassis, modules, or virtual contexts.

Procedure

Step 1 Choose **Config > Devices > All Devices**.

The Device Management window appears.

Step 2 In the device tree or in the All Devices table, click **Add**.

The New Device window appears.

Step 3 Enter the information for the device using the information in Table 4-2.

Table 4-2 New Device Attributes

Field	Description
Name	Unique name for the device. Valid entries are unquoted text strings with no spaces and a maximum of 26 alphanumeric characters.
Model	Type of device to import: • ACE 4710—An ACE 4710 appliance. • CSS—A Cisco Content Services Switch. • Cisco IOS Device—A supported Catalyst 6500 series chassis, Cisco 7600 series router, or VSS device. • GSS—A high end device that monitors the health and load of the server load balancers in each of your data centers and then uses that information along with customer-controlled routing algorithms to choose the best-suited and least-loaded data center in real time.
Primary IP	IP address for the device in dotted-decimal format.
Access Protocol	Field that appears when you select CSS, GSS or IOS Device for the model. Choose Secure/SSH2 or Telnet as the protocol that ANM uses to access the device for Cisco IOS devices. GSS uses Secure/SSH2 (that is the only option that appears).
User Name	Account name for device access. **Note** If you did not configure an account on the chassis before starting this procedure, you can enter an alphanumeric string with no spaces to complete this procedure. However, we recommend that you configure an account on the device to prevent unauthorized access.
Password	Password for the account.

Table 4-2 New Device Attributes (continued)

Field	Description
Enable Password	Field that appears for Catalyst 6500 series chassis, Cisco 7600 series routers, and GSS devices for an extra level of security.
SNMP v2c Enabled	Field that appears for Catalyst 6500 series chassis, Cisco 7600 series routers, and CSS. Check the SNMP v2c Enabled checkbox to configure SNMP access.
SNMP v2c Read-Only Community String	SNMPv2c community string to be used.
Description	Field that appears if you check the SNMP v2c Enabled checkbox. Enter the community string for the device. **Note** If you are adding a Catalyst 6500 series chassis, in the Community field, enter the SNMP community string already configured on the Catalyst 6500 series chassis. ANM uses this string to query device status information such as VLAN and interface status. This SNMP community string is also used for any CSM modules contained in the specified Catalyst 6500 series chassis. For Catalyst 6500 series chassis, CSS, and CSM devices, the SNMP community string already configured on the device is used by ANM for polling. For ACE modules and ACE appliances, the SNMP community string entered into ANM is configured on the ACE module/appliance and is used for polling the devices.

Step 4 Do one of the following:

- Click **Next** to save your entries and import device information:
  - If no ACE modules are associated with the device, a progress bar reports status, and the All Devices table refreshes with updated information.
  - If ACE modules are associated with the device, a progress bar reports status, and the Modules configuration window appears. Skip to Step 5.
- Click **Cancel** to exit the procedure without saving your entries and to return to the All Devices table. Clicking Cancel prevents device information from being imported and prevents ACE module discovery.

Step 5 In the Modules window, you can either import the current module or click **Next** to skip this module and continue with the next module.

Step 6 To import a module, in the Card Slot field, confirm that the correct module appears.

Step 7 In the Card Type field, confirm that the correct device type appears.

Note The device version supported will also appear, but only by major release. For example, 8.2x might be supported but only 8.2 will display.

You will see but cannot revise the *Module has been imported into* ANM field. Confirm that the checkbox is checked to indicate that the module has already been imported or cleared to indicate that it has not been imported. This is a read-only field.

Step 8 In the Operation to Perform field, choose one of the following:

- **Import**—ANM is to import the ACE module configuration. Skip to Step 9.

- **Perform Initial Setup And Import**—Allows you to perform initial setup manually required for ANM to communicate with the ACE module and imports ACE module configuration. Skip to Step 10.

Note We recommend that you choose this option for ACE modules that are configured only with factory defaults.

Step 9 If you choose Import, enter the following information:

a. In the Admin Context IP field, enter the IP address to use for this module.

b. Specify whether the ACE module is configured with the factory-default admin credentials (admin/admin):

- If you have changed the default admin credentials, enter the new device credentials in the User Name and Password fields.
- If you have not changed the default admin credentials (admin/admin), enter the new admin credentials in the User Name and Password fields, and ANM will configure the credentials on the ACE.

Note For security reasons, we recommend that you change the username and password on your ACE device (and modules) after you import them. The security on your ACE module can be compromised because the administrative username and password are configured to be the same for every ACE module shipped from Cisco. See the "Changing ACE Module Passwords" procedure on page 4-65.

c. In the User Name field, enter the username for accessing this module. Valid entries are unquoted text strings with a maximum of 24 characters.

d. In the Password field, enter the password for accessing this module. Reenter the password in the Confirm field. Valid entries are unquoted text strings with a maximum of 64 characters.

Step 10 If you choose Perform Initial Setup And Import, enter the following information:

a. In the Host Name field, enter a unique name for this module. Valid entries are alphanumeric strings with no spaces and a maximum of 32 characters.

b. In the Admin Context IP field, enter the IP address for this module.

c. In the Netmask field, from the drop-down list, choose the subnet mask to apply to this IP address.

d. In the Gateway field, enter the IP address of the gateway router to use.

e. In the VLAN field, choose the VLAN to which this module belongs.

f. Specify whether the ACE blade is configured with the factory-default admin credentials (admin/admin):

- If you have changed the default admin credentials, enter the new device credentials in the User Name and Password fields.
- If you have not changed the default admin credentials (admin/admin), enter new admin credentials in the User Name and Password fields, and ANM will configure the credentials on the ACE.

Note For security reasons, we recommend that you change the username and password on your ACE device (and modules) after you import them. The security on your ACE module can be compromised because the administrative username and password are configured to be the same for every ACE module shipped from Cisco. See the "Changing ACE Module Passwords" procedure on page 4-65.

g. In the User Name field, enter the username for accessing this module. Valid entries are unquoted text strings with a maximum of 24 characters.

h. In the Password field, enter the password for accessing this module. Reenter the password in the Confirm field. Valid entries are unquoted text strings with a maximum of 64 characters.

Step 11 Do one of the following:

- Click **OK** to save your entries and to continue with the device configuration. A progress bar reports status and the Device configuration window appears.
- Click **Cancel** to exit the procedure without importing ACE modules and to return to the All Devices table.

Note Clicking Cancel in this window does not cancel the chassis importing process.

Step 12 (Optional) To confirm that the virtual contexts on the ACE were successfully imported into ANM, do the following:

a. Choose **Config > Devices**. The device tree appears.

b. In the device tree, choose the ACE that you just imported. The Virtual Contexts table appears, listing the contexts for that device.

c. Confirm that the contexts imported successfully:

- If *OK* appears in the Config Status column, it means that the context imported successfully.
- If *Import Failed* appears in the Config Status column, it means that the context did not import successfully.

d. To synchronize the configurations for the context import that failed, choose the context, and then click **Sync**. ANM will synchronize the context by uploading it from the ACE device.

For more information on synchronizing virtual contexts, see the "Creating Virtual Contexts" procedure on page 5-2.

Note If you receive authentication errors or incorrect username/password errors when trying to import ACE devices, refer to the ACE documentation regarding username and password settings and limitations.

Tip After you add an ACE device, see the "Enabling a Setup Syslog for Autosync for Use With an ACE" section on page 4-20 to enable auto sync, which allows ANM to synchronization with the ACE CLI when ANM receives a syslog message from the ACE rather wait the default polling period.

Adding ACE Modules to ANM

You can add ACE modules into the ANM database at any time after the host chassis, VSS, or router has been added.

Before You Begin

- Ensure that the module to be imported has booted successfully and is in OK/Pass state. To check the module state, enter the **show module** Supervisor IOS CLI command.
- Note that time needed to import ACE modules depends on the number of modules and contexts that you are importing. For example, an ACE module with 20 virtual contexts takes longer than an ACE module with 5 contexts. While ANM imports the module, you cannot perform other activities in the same session. You can, however, establish a new session with the ANM server and perform activities on other devices, modules, or virtual contexts.
- If you receive authentication errors or incorrect username/password errors when you try to import an ACE module, see the ACE documentation regarding username and password settings and limitations.
- If you physically replace an ACE module in a chassis, you need to synchronize the chassis in ANM. We recommend you start by adjusting syslog settings to facilitate the ANM auto synchronization process as described in the "Enabling a Setup Syslog for Autosync for Use With an ACE" section on page 4-20.

Assumptions

You have added to the ANM database, at least one host chassis, VSS, or router that contains the ACE modules. For information about adding the host device, see the "Adding Devices to ANM" section on page 4-9.

Restrictions

ANM 3.0 and greater releases do not support the importing of an ACE module that contains an A1(6.x) software release or an ACE appliance that contains an A1(7.x) or A1(8.x) software release. If you attempt to import an ACE that supports one of these releases, ANM displays a message to instruct you that it failed to import the unrecognized ACE configuration and that device discovery failed.

However, if you perform an ANM upgrade (for example, from ANM 2.2 to ANM 3.0), and the earlier ANM release contained an inventory with an ACE module that supported the A1(6x) software release or an ACE appliance that supported the A1(7.x) or A1(8.x) software release, ANM 3.0 (and greater) allows the A1(x) software release to reside in the ANM database and will support operations for the release. ANM prevents a new import of an ACE module or ACE appliance that contains the unsupported software version.

We strongly recommend that you upgrade your ACE module or ACE appliance to a supported ACE software release, and that you instruct ANM to recognize the updated release. See the "Instructing ANM to Recognize an ACE Module Software Upgrade" section on page 4-16.

See the *Supported Device Tables for the Cisco Application Networking Manager 3.0* for a complete list of supported ACE module and ACE appliance software releases.

Procedure

Step 1 Choose **Config > Devices > All Devices**.

The All Devices table appears.

Step 2 In the All Devices table, choose the host device that contains the ACE module you want to import, and then click **Modules**.

The Modules table appears.

Step 3 In the Modules table, choose the module you want to import, and then click **Import**.

The Modules configuration window appears.

Step 4 In the Card Slot field, confirm that the correct module appears.

Step 5 In the Card Type field, confirm that the correct version appears.

Step 6 In the Operation to Perform field, choose the import option:

- **Import**—ANM is to import the ACE module configuration. Skip to Step 7.
- **Perform Initial Setup And Import**—ANM is to provide the ACE module with a prediscovery configuration file and then import the ACE module configuration.

  Choose this option only if the ACE module has never been configured before.

  Specify whether the ACE module is configured with the factory-default admin credentials (admin/admin):

  – If you have changed the default admin credentials, enter the new device credentials in the User Name and Password fields.

  – If you have not changed the default admin credentials (admin/admin), enter new admin credentials in the User Name and Password fields, and ANM will configure the credentials on the ACE.

  Skip to Step 8.

Step 7 If you choose Import, enter the following information:

a. In the Admin Context IP field, enter the IP address to use for this module.

b. In the User Name field, enter the username for accessing this module.

c. In the Password field, enter the password for accessing this module.

Note For security reasons, we recommend that you change the username and password on your ACE modules after you import them. The security on your ACE module can be compromised because the administrative username and password are configured to be the same for every ACE module shipped from Cisco. See the "Changing ACE Module Passwords" procedure on page 4-65.

Step 8 If you chose Perform Initial Setup And Import, enter the following information:

a. In the Host Name field, enter a unique name for the module. Valid entries are alphanumeric strings with no spaces and a maximum of 32 characters.

b. In the Admin Context IP field, enter the IP address for the module.

c. In the Netmask field, from the drop-down list, choose the subnet mask to apply to the IP address.

d. In the Gateway field, enter the IP address of the gateway router.

e. In the VLAN field, choose the VLAN to which the module belongs.

Step 9 Do one of the following:

- Click **OK** to save your entries. A progress bar reports status and the Modules table refreshes with updated information.

- Click **Cancel** to exit the procedure without importing the module and to return to the Modules table.

Step 10 (Optional) To confirm that the virtual contexts on the module were successfully imported into ANM:

a. Choose **Config > Devices**. The device tree appears.

b. In the device tree, choose the module that you just imported. The Virtual Contexts table appears, listing the contexts for that module.

c. Confirm that the contexts imported successfully:

   – If *OK* appears in the Config Status column, it means that the context imported successfully.

   – If *Import Failed* appears in the Config Status column, it means that the context did not import successfully.

d. To synchronize the configurations for the context import that failed, choose the context, and then click **Sync**. ANM will synchronize the context by uploading it from the module.

   For more information on synchronizing virtual contexts, see the "Creating Virtual Contexts" procedure on page 5-2.

Tip After you add ACE devices, see the "Enabling a Setup Syslog for Autosync for Use With an ACE" section on page 4-20 to enable auto sync, which allows ANM to synchronization with the ACE CLI when ANM receives a syslog message from the ACE rather wait the default polling period.

Related Topics

- Instructing ANM to Recognize an ACE Module Software Upgrade, page 4-16
- Changing ACE Module Passwords, page 4-65
- Removing Modules from the ANM Database, page 4-69
- Synchronizing Module Configurations, page 4-59

Instructing ANM to Recognize an ACE Module Software Upgrade

After you import an ACE module into the ANM database and the ACE module software version has been upgraded on Cisco.com, perform the procedure outlined in this section to enable ANM to recognize the updated release and display features and functions in the ANM GUI that are appropriate for the latest ACE module software release.

For example, if an imported ACE module contains software release A2(2.1), and you wish to upgrade to software release A2(3.0) to take advantage of features such as backup and restore, you must perform the steps outlined below to instruct ANM to recognize the upgraded ACE module software version and display the features and functions associated with this release. If you do not instruct ANM to recognize an ACE module software upgrade, the ACE module import will occur without issue but the new features and functions associated a specific ACE module software release will not appear in the ANM GUI.

Assumption

You have added to the ANM database, at least one host chassis, VSS, or router that contains the ACE modules. For information about adding the host device, see the "Adding Devices to ANM" section on page 4-9.

Procedure

Step 1 When you upgrade an ACE module software image, after you complete the upgrade process perform a CLI sync on the chassis, VSS, or router that contains the ACE module. Perform the procedure outlined in Synchronizing Chassis Configurations, page 4-59.

Step 2 After you complete the CLI sync, whenever ANM detects an upgrade on an imported ACE module, ANM issues a warning to instruct you to perform a CLI sync on the ACE module to recognize the upgrade. Perform the procedure outlined in Synchronizing Module Configurations, page 4-59.

The ACE software upgrade sequence is completed.

Importing CSM Devices

You can import CSM devices into the ANM database at any time after the host chassis or router has been imported.

Note ANM assigns the device type CSM to both CSM and CSM-S devices. This assignment has to do with how ANM collects and assigns the information that it receives from the device and does not affect functionality. To differentiate between these devices, see the description information in the user interface.

Assumption

You have added to the ANM database, at least one host chassis or router that contains the CSM. For information about adding the host device, see the "Adding Devices to ANM" section on page 4-9.

Procedure

Step 1 Choose **Config > Devices > All Devices**.

The All Devices table appears.

Step 2 In the All Devices table, choose the host device that contains the CSM that you want to import, and then click **Modules**.

The Modules table appears.

Step 3 In the Modules table, choose the CSM that you want to import, and then click **Import**.

The Modules configuration window appears.

Step 4 Verify that the information is correct in the following read-only fields:

- Card Slot—The slot in the chassis in which the module resides.
- Card Type—The device type; in this instance, CSM.
- Module Has Been Imported Into ANM—The checkbox is checked to indicate that the module has already been imported or cleared to indicate that it has not been imported.

Step 5 In the Operation to Perform field, choose **Import**.

Step 6 Do one of the following:

- Click **OK** to save your entries. A progress bar reports status and the Modules table refreshes with updated information.

- Click **Cancel** to exit the procedure without importing the device and to return to the Modules table.

Related Topics

- Removing Modules from the ANM Database, page 4-69
- Synchronizing Module Configurations, page 4-59

Importing GSS Devices

You use GSS devices in a network to provide distributed and redundant global server load balancing (GSLB) domain name system (DNS) services. The network of GSS devices, or GSS cluster, consists of a primary Global Site Selector Manager (GSSM), a standby GSSM, and GSS devices. You can create GSLB DNS services by first performing a basic configuration of each device, and then access the primary GSSM to manage the centralized and shared GSLB configuration.

Follow these guidelines for importing GSS devices into ANM:

- You only need to import the primary GSSM into ANM—You are not required or permitted to add either the standby GSSM or GSS device. ANM communicates only with the primary GSSM for activation and suspension of DNS rules and virtual IP (VIP) answers, and for collecting statistics.
- GSS graphical user interface (GUI) and CLI must have matching passwords—The username that you configure while adding a GSS device to ANM, must be the same on both the GSS GUI and GSS CLI.
- Communication between ANM and the primary GSSM is accomplished using GSS Communication Ethernet Interface—This interface is used for internal communication between the primary GSSM and the other GSS devices in the GSS cluster.

When you configure your GSS for deployment behind a firewall, you must allow DNS traffic into the device. If you have multiple GSS devices deployed so that traffic between the devices must pass through a firewall, configure the firewall to allow inter-GSS communications and inter-GSS status reporting. Depending on your GSS configuration, you can also allow other traffic to pass through the firewall. This requirement depends on your GSS configuration (for example, if you are using TCP-based or KAL-AP keepalives) and the ability to access certain GSS services through the firewall (for example, SNMP).

The GSS does not support deployment of devices behind a network address translation (NAT) system for inter-GSS communication. The communication between the GSS devices cannot include an intermediate device behind a NAT because the actual IP address of the devices is embedded in the payload of the packets. For more information, see the GSS documentation on Cisco.com.

Table 4-3 lists the TCP ports that are used by ANM to communicate with GSS.

Table 4-3 TCP Ports Used by ANM for GSS

Port	Description
22	SSH
2001	Java RMI
3009	Secure RMI

Note Terminal length settings will be set to 0 during import, synchronization, and background polling. The previous terminal length settings you had before import, synchronization, and background polling is performed will not be preserved.

Procedure

Step 1 Choose **Config > Devices > All Devices**.

The All Devices table appears.

Step 2 In the All Devices table, choose the **Add** button.

The New Device window appears.

Step 3 In New Device window, configure the device using the information in Table 4-4.

Table 4-4 GSS Configuration Options

Field	Description
Name	Name assigned to the device.
Model	Drop-down list from which you can choose GSS.
Primary IP Address	Read-only field with the device IP address.
User Name	Account name for device access.
Password	Password for this user account (configurable, based on minimum and maximum values defined).
Enable Password	Field that appears for Catalyst 6500 series chassis, Cisco 7600 series routers, CSS, and GSS devices to provide an extra level of security. **Note** When a GSS is configured with remote authorization using the **enable** command in the user privilege, the enable password is not used.
Description	Brief description for this device.

Step 4 Do one of the following:

- Click **OK** to save your entries. A progress bar reports status and the Modules table refreshes with updated information.
- Click **Cancel** to exit the procedure without importing the device and to return to the Modules table.

Importing VSS 1440 Devices

Catalyst 6500 Virtual Switching Systems (VSS) 1440 devices allow for the combination of two switches into a single, logical network entity from the network control plane and management perspectives. To the neighboring devices, the Cisco Virtual Switching System appears as a single, logical switch or router.

VSS devices will be discovered as a normal Cisco IOS device in ANM if the device is already converted to virtual switch mode.

Note ANM does not recognize failure scenarios as discussed in the "Configuring Virtual Switching System" section of the "*Catalyst 6500 Release 12.2SXH and Later Software Configuration Guide*" on Cisco.com at http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/vss.html#wp1062314.

Enabling a Setup Syslog for Autosync for Use With an ACE

You can set up auto synchronization to occur when ANM receives a syslog message from ACE devices. This feature allows a faster, more streamlined synchronization process between ANM and any out-of-band configuration changes. Rather than wait the default polling period, ANM will synchronize when a syslog message is received if you enable the Autosync feature.

Note ANM does not support Autosync for GSS devices.

Procedure

Step 1 Choose **Config > Devices**. From the device tree, select either an ACE module or an ACE appliance.

Step 2 Choose **Setup Syslog for Autosync**.

The Setup Syslog for Autosync window appears.

Step 3 Choose one or more virtual contexts for which you want to receive Autosync syslog messages.

Step 4 Click the **Setup Syslog** button.

A progress bar window appears.

The following CLI commands are sent to the enabled ACE devices:

```
logging enable
logging trap 2
logging device-id string <ACE-Ip>/Admin
logging host <ANM-Ip>  udp/514
logging message 111008 level 2
```

Step 5 If the setup is successful, a checkbox with check mark will appear in the Setup Syslog for Autosync? column for each virtual context that you selected. If there are any errors, the errors will be shown in a pop-up window.

Discovering Large Numbers of Devices Using IP Discovery

The IP Discovery feature allows you to discover and import chassis and ACEs into the ANM database as follows:

1. Preparing devices for discovery. This process involves enabling SSH and XML over HTTPS and adding device credentials. See the "Preparing Devices for IP Discovery" section on page 4-21.
2. Discovering devices residing on your network. The ANM uses SSH, XML over HTTPS, and Telnet to discover its supported devices. When you run IP Discovery, you locate IP addresses of ACE chassis and appliances. See the "Running IP Discovery to Identify Devices" section on page 4-24.

   After discovery, devices do not appear in the Devices table until device import is completed. To import a specific chassis into the ANM database, you need to enter IP and credentials information for the chassis and then import it and any associated modules. While this discovery method requires you to add more information initially, it provides more control over the discovery process.
3. Importing the device information into the ANM database to add the device into the Devices table. See the "Adding Network Devices into ANM" section on page 4-9.
4. After importing a module host device, such as a Catalyst 6500 series chassis, you can add ACE modules and CSMs into the ANM database. See the "Adding ACE Modules to ANM" section on page 4-14 or the "Importing CSM Devices" section on page 4-17.
5. After you start a discovery job, you can monitor its status. See the "Monitoring IP Discovery Status" section on page 4-26.

ANM offers multiple ways to accomplish some of these steps. For example, you can either run a discovery job to identify the available chassis, and then choose the ones to import, or you can import a specific chassis into the ANM database.

To add a chassis without running discovery, see the "Adding Devices to ANM" section on page 4-9.

See the *Supported Devices Table for Cisco Application Networking Manager 3.0* for more information about the devices that ANM supports.

This section contains the following topics:

- Preparing Devices for IP Discovery, page 4-21
- Running IP Discovery to Identify Devices, page 4-24
- Monitoring IP Discovery Status, page 4-26

Preparing Devices for IP Discovery

This section describes how to prepare your Cisco devices for IP Discovery by enabling SSH and Telnet on each device and by configuring device SSH and Telnet credentials though ANM. These tasks enable ANM to communicate with the devices and collect data from them.

Caution IP Discovery sends unencrpyted credentials (Telnet and SNMP) to all devices on the specified subnet who respond to the associated ports. This is a potential security risk because credentials are broadcast out to one or more networks. IP Discovery may also find devices that cannot be imported or may not be able to locate devices that could be imported.

Before You Begin

Ensure that you have enabled SSH and Telnet in your Cisco network devices by performing the tasks described in the following sections:

- Enabling SSH or Telnet Access on Catalyst 6500 Series Switches and Cisco 7600 Series Routers, page 4-4
- Enabling SSH Access and the HTTPS Interface on the ACE Module and Appliance, page 4-5

This section contains the following topics:

- Configuring Device Access Credentials, page 4-22
- Modifying Credential Pools, page 4-23

Configuring Device Access Credentials

You can add device credentials to ANM before running IP Discovery.

Procedure

Step 1 Choose **Config > Tools > Credential Pool Management**.

The New Credential Pool window appears.

Step 2 In the Name field, enter the name of the new credential pool.

Step 3 Click **Save** to save this entry and to proceed with credentials configuration.

The configuration window appears.

Step 4 Set the Telnet credentials as follows:

a. Choose **Configuration > Telnet Credentials**. The Telnet Credentials table appears.

b. In the table, click **Add** to add a set of credentials to this credential pool, or choose an existing set of credentials, and click **Edit** to modify it.

c. Enter the credentials (see Table 4-5).

Table 4-5 Telnet Credentials

Field	Description
IP Address	Specific IP address in dotted-decimal notation or use an asterisk (*) as a wildcard character to identify a number of devices, such as 192.168.11.*.
User Name	Telnet username for the specified devices.
Password	Telnet password for the specified devices.
Confirm	Telnet password that you reenter.
Enable Password	Telnet enable password for the specified devices. ANM uses this password during the Catalyst 6500 series chassis and Catalyst 6500 Virtual Switching System (VSS) 1440 import process.
Confirm	Telnet enable password that you reeenter.

d. Do one of the following:

- Click **OK** to save your entries and to return to the Telnet Credentials table.
- Click **Cancel** to exit this procedure without saving your entries and to return to the Telnet Credentials table.

– Click **Next** to deploy your entries and to add another set of Telnet credentials.

Step 5 Set the SNMP credentials as follows:

a. Choose **Configuration > SNMP Credentials**. The SNMP Credentials table appears.

b. Click **Add** to add a set of credentials to this credential pool, or choose an existing set of credentials, and click **Edit** to modify it.

c. Enter the SNMP credentials (see Table 4-6).

Table 4-6 SNMP Credentials

Field	Description
IP Address	Specific IP address in dotted-decimal notation is used or an asterisk (*) is used as a wildcard character to identify a number of devices, such as 192.168.11.*.
Mode	Default version of SNMP is selected for this credential pool. Snmpv2 indicates that SNMP version 2 is to be used for this credential pool for the specified devices.
RO Community	SNMP read-only string for the specified devices. This entry is case sensitive.
Timeout	Time, in seconds, that the ANM is to wait for response from a device before performing the first retry.
Retries	Number of times that the ANM is to attempt to communicate with a device before declaring that the device has timed out.

Step 6 Do one of the following:

- Click **OK** to save your entries and to return to the SNMP Credentials table.
- Click **Cancel** to exit without saving your entries and to return to the SNMP Credentials table.
- Click **Next** to deploy your entries and to configure another set of SNMP credentials.

After establishing the Telnet and SNMP credentials, you are ready to run IP Discovery. See the "Running IP Discovery to Identify Devices" section on page 4-24.

Related Topics

- Running IP Discovery to Identify Devices, page 4-24
- Configuring Device Access Credentials, page 4-22
- Discovering Large Numbers of Devices Using IP Discovery, page 4-21

Modifying Credential Pools

You can modify existing Telnet or SNMP credentials.

Procedure

Step 1 Choose **Config > Tools > Credential Pool Management**.

The Credential Pools configuration window appears.

Step 2 Choose the credential pool that you want to modify.

The Edit Credential Pool configuration window appears.

Step 3 Click **Edit**.

Step 4 To modify the existing Telnet credentials, do the following:

a. Choose **Configuration > Telnet Credentials**. The Telnet Credentials table appears.

b. In the table, click **Add** to add a set of credentials to this credential pool, or choose an existing set of credentials, and click **Edit** to modify it.

c. Enter the Telnet credentials (see Table 4-5).

d. Do one of the following:

- Click **OK** to save your entries and to return to the Telnet Credentials table.
- Click **Cancel** to exit this procedure without saving your entries and to return to the Telnet Credentials table.
- Click **Next** to deploy your entries and to add another set of Telnet credentials.

Step 5 To modify the existing SNMP credentials, do the following:

a. Choose **Configuration > SNMP Credentials**. The SNMP Credentials table appears.

b. Click **Add** to add a set of credentials to this credential pool, or choose an existing set of credentials, and click **Edit** to modify it.

c. Enter the SNMP credentials (see Table 4-6).

d. Do one of the following:

- Click **OK** to save your entries and to return to the SNMP Credentials table.
- Click **Cancel** to exit without saving your entries and to return to the SNMP Credentials table.
- Click **Next** to deploy your entries and to configure another set of SNMP credentials.

Related Topics

- Running IP Discovery to Identify Devices, page 4-24
- Configuring Device Access Credentials, page 4-22
- Discovering Large Numbers of Devices Using IP Discovery, page 4-21

Running IP Discovery to Identify Devices

You can run IP Discovery to locate IP addresses of the Catalyst 6500 series chassis (hosting the ACE module), ACE appliance, and Catalyst 6500 Virtual Switching System (VSS) devices.

After establishing Telnet and SNMP credentials (see the "Configuring Device Access Credentials" section on page 4-22), use this procedure to identify chassis and ACEs on your network.

Caution IP Discovery sends unencrpyted credentials (Telnet and SNMP) to all devices on the specified subnet that respond to the associated ports. This is a potential security risk because credentials are broadcast out to one or more networks. IP Discovery may also find devices that cannot be imported or be unable to find devices that could be imported.

Before You Begin

For this procedure, you need the follow items:

- IP address for the discovery process.
- Applicable subnet mask.
- Valid credentials for this discovery (see the "Configuring Device Access Credentials" section on page 4-22).
- Verification that the devices have SSH enabled (see the "Preparing Devices for IP Discovery" section on page 4-21).

Procedure

Step 1 Choose **Config > Tools > IP Discovery**.

The Discovery Jobs table appears.

Tip If you already know the IP address of your devices, use the Config > Devices > Add function. See the "Adding Network Devices into ANM" section on page 4-9.

Step 2 To create a discovery job, click **Add**.

The Discovery Jobs window appears.

Step 3 In the IP Address field, enter the IP address of a specific device in dotted-decimal notation such as 192.168.11.1.

Step 4 In the Netmask field, choose the subnet mask to be used. When you specify a subnet mask, the discovery process discovers all devices in the range of the IP address and its subnet mask. The default netmask is 255.255.255.0.

Note Choose a higher subnet mask only if you are certain that it is appropriate for your network and you understand the impact. If you choose the subnet mask for a class A or class B network, the discovery process becomes extensive and can take a substantial amount of time to complete.

Step 5 In the Credential Pool field, choose the credential pool to be used for this discovery.

Step 6 Click **Discover** to run discovery now or **Cancel** to exit this procedure without running discovery.

When you run IP Discovery, the Discovery Jobs table reflects the state of the discovery as it runs. The amount of time to finish a discovery job depends on the size of your network and network activity.

If necessary, click **Stop** to stop the discovery process. When the process has stopped, the Discovery Jobs table appears with the discovery job in the table with the state *Aborted*.

Tip Click **Refresh** during IP Discovery to see the number of devices found as the discovery process progresses.

Step 7 (Optional) View the discovery process status (see the "Monitoring IP Discovery Status" section on page 4-26).

Step 8 (Optional) Import ACE devices into the ANM when the discovery process is complete (see the "Adding Network Devices into ANM" section on page 4-9).

Related Topics

- Creating Virtual Contexts, page 5-2
- Adding and Managing Devices, page 4-1
- Using Configuration Building Blocks, page 15-1

Monitoring IP Discovery Status

You can monitor device discovery status after starting a discovery job.

Procedure

Step 1 Click **Config > Tools > IP Discovery**.

The Discovery Jobs table appears with the following information for each discovery job:

- IP address
- Subnet mask
- Start Time in the format *hh:mm:ss.nnn*
- End Time, if available, in the format *hh:mm:ss.nnn*
- Credential Pool being used
- State of the discovery job, such as *Running* or *Completed*
- Number of devices found

Step 2 Locate your discovery job to see its current status.

If necessary, click **Stop** to stop the discovery process. When the process has stopped, the Discovery Jobs table appears with the discovery job in the table with the state *Aborted*.

Step 3 When discovery is complete, choose the discovery job in the table. A list of the discovered devices appears below the Discovery Jobs table.

You can now populate the ANM with chassis and ACEs. See the "Adding Network Devices into ANM" section on page 4-9.

Related Topics

- Adding Network Devices into ANM, page 4-9
- Running IP Discovery to Identify Devices, page 4-24
- Information About Importing Devices, page 4-3

Configuring Devices

This section describes how to configure the devices that you add to ANM and includes the following topics:

- Configuring Device System Attributes, page 4-27
- Configuring Catalyst 6500 Series Chassis or Cisco 7600 Series Router Interfaces, page 4-34
- Managing Catalyst 6500 Series Chassis or Cisco 7600 Series Router VLANs, page 4-40

Note The ANM does not detect changes made to a chassis device though the CLI. Be sure to synchronize chassis configurations whenever chassis configuration has been modified via the CLI.

Configuring Device System Attributes

This section shows how to configure the device system attributes. For the CSM, CSS, and GSS devices, the system attributes consist of the primary attributes only. For the Catalyst 6500 series chassis, Catalyst 6500 Virtual Switching System (VSS) 1440 devices, and Cisco 7600 series routers, the system attributes also include the static route attributes.

This section includes the following topics:

- Configuring CSM Primary Attributes
- Configuring CSS Primary Attributes
- Configuring GSS Primary Attributes
- Configuring Catalyst 6500 VSS 1440 Primary Attributes
- Configuring Catalyst 6500 Series Chassis and Cisco 7600 Series Router Primary Attributes
- Configuring Catalyst 6500 Series Chassis, Catalyst 6500 Virtual Switching System 1440 Devices, and Cisco 7600 Series Routers Static Routes

Configuring CSM Primary Attributes

You can configure primary attributes for CSM devices.

Procedure

Step 1 Choose **Config > Devices > All Devices**.

The device tree appears.

Step 2 In the device tree, choose the CSM that you want to configure, and then choose **System > Primary Attributes**.

The Primary Attributes window appears.

Step 3 In the Description field, enter a brief description of the module.

Step 4 Choose another CSM for high availability pairing from the Redundant Device field, which displays any other CSM devices that have been imported into ANM.

Step 5 Click **Deploy Now** to deploy this configuration on the CSM and save your entries to the running-configuration and startup-configuration files.

To exit this procedure without deploying your entries, choose another device in the device tree or in the object selector above the configuration pane.

Related Topics

- Configuring Devices, page 4-27
- Adding ACE Modules to ANM, page 4-14

Configuring CSS Primary Attributes

You can configure primary attributes for CSS devices.

Procedure

Step 1 Choose **Config > Devices > All Devices**.

The All Devices table appears.

Step 2 In the All Devices table, choose the CSS that you want to configure, and then choose **System > Primary Attributes**.

The Primary Attributes window appears with information about the device.

Step 3 Configure the CSS using the information in Table 4-7.

Note Most of the information is read directly from the device during the import process and cannot be changed using the ANM interface.

Table 4-7 CSS Primary Attributes Configuration Options

Field	Description
Description	Brief description for this device.
Device Type	Read-only field that has the device type in gray.
Use Telnet	Read-only field that will be checked if the device was imported using Telnet.
IP Address	Read-only field with the device IP address.
Redundant Device	Field that displays any other CSS devices that have been imported into the ANM database. Choose another CSS for high availability pairing.

Table 4-7 CSS Primary Attributes Configuration Options (continued)

Field	Description
SNMP v2c Enabled	Checkbox to enable SNMP version 2c access. Uncheck the checkbox to disable this feature. If you enable this feature, in the SNMP Trap Community string field, enter the SNMP community string.
SNMP v3 Enabled	Checkbox to enable SNMP Version 3 access. Uncheck the checkbox to disable this feature. If you enable this feature, do the following: 1. In the SNMP V3 User Name field, enter the SNMP username. 2. In the SNMP V3 Mode field, choose the level of security to be used when accessing the chassis: • NoAuthNoPriv—SNMP uses neither authentication nor encryption in its communications. • AuthNoPriv—SNMP uses authentication, but the data is not encrypted. 3. If you choose AuthNoPriv, do the following: a. In the SNMP V3 Auth Proto field, choose MD5 or DES to specify the authentication mechanism. b. In the SNMP V3 Auth Pass field, enter the user authentication password. Valid entries are unquoted text strings with no spaces and a maximum of 130 characters. c. In the Confirm field, reenter the user authentication password.

Step 4 Click **Deploy Now** to deploy this configuration on the CSS and to save your entries to the running-configuration and startup-configuration files.

To exit this procedure without deploying your entries, choose another device in the device tree or in the object selector above the configuration pane.

Related Topics

- Configuring Devices, page 4-27
- Adding Network Devices into ANM, page 4-9

Configuring GSS Primary Attributes

You can configure primary attributes for Cisco Global Site Selector devices.

Procedure

Step 1 Choose **Config > Devices > All Devices**.

The All Devices table appears.

Step 2 In the All Devices table, choose the GSS that you want to configure, and then choose **System > Primary Attributes**.

The Primary Attributes window appears with information about the device.

Step 3 Configure the GSS using the information in Table 4-8.

Table 4-8 GSS Primary Attributes Configuration Options

Field	Description
Description	Brief description for this device.
Device Type	Read-only field that has the device type, in this case GSS, in gray.
IP Address	Device IP address.

Step 4 (Optional) To update the IP address and/or password for the GSS on the ANM server only, click **Update IP Address/Password**.

The Update IP Address/Password window appears.

Note The password changes are for the ANM server only. The Password/Enable password on the device will not be changed.

Enter new credentials in the Update IP Address/Password window using the information in Table 4-9.

Table 4-9 GSS Change IP Address and Password Options

Field	Description
Old Primary IP Address	Read-only field displaying the device IP address.
New Primary IP Address	IP address that you wish to have GSS associated with on the server.
Update	Available password update choices are as follows: • **Both**—Update both the password and enable passwords. • **Enable Password Only**—Update only the enable password. • **Password Only**—Update only the password.
New Password	New password.
Confirm New Password	New password that you reenter.
New Enable Password	New enable password.
Confirm New Enable Password	New enable password that you reenter.

Step 5 Do one of the following:

- Click **OK** to save any changes made to GSS server IP address or password to the ANM server.
- Click **Cancel**.

You return to the Primary Attributes Page.

Step 6 Click **Deploy Now** to deploy this configuration save your entries to the gslb-configuration file.

To exit this procedure without deploying your entries, choose another device in the device tree or in the object selector above the configuration pane.

Related Topics

- Configuring Devices, page 4-27
- Adding Devices to ANM, page 4-9
- Adding Network Devices into ANM, page 4-9

Configuring Catalyst 6500 VSS 1440 Primary Attributes

You can configure primary attributes for VSS devices.

Procedure

Step 1 Choose **Config > Devices > All Devices**.

The device tree appears.

Step 2 In the device tree, choose the device you want to configure, then choose **System > Primary Attributes**. The Primary Attributes window appears with information about the chassis.

Most of the information is read directly from the device during the import process and cannot be changed using the ANM interface. For example, a VSS-enabled checkbox will display as a read-only field. You can, however, add a description and configure the device for SNMPv2 or SNMPv3 access.

Note For the ACE devices in VSS, the slot number is represented in the format switch number/slot number.

Step 3 In the Description field, enter a brief description for the device.

Step 4 To enable SNMPv2c access, do the following:

a. Check the SNMPv2c Enabled checkbox.

b. In the SNMP Trap Community string field, enter the SNMP community string.

Step 5 Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files. You return to the All Devices table.

Related Topics

- Displaying Chassis Interfaces and Configuring High-Level Interface Attributes, page 4-34
- Displaying Modules by Chassis, page 4-68
- Managing Catalyst 6500 Series Chassis or Cisco 7600 Series Router VLANs, page 4-40

Configuring Catalyst 6500 Series Chassis and Cisco 7600 Series Router Primary Attributes

You can configure primary attributes for Catalyst 6500 series chassis and Cisco 7600 series routers.

Procedure

Step 1 Choose **Config > Devices > All Devices**.

The device tree appears.

Step 2 In the device tree, choose the device that you want to configure, and choose **System > Primary Attributes**.

The Primary Attributes window appears.

Most of the information is read directly from the device during the import process and cannot be changed using the ANM interface. However, you can add a description and configure the device for SNMPv2 or SNMPv3 access.

Step 3 In the Description field, enter a brief description for the device.

Step 4 To enable SNMPv2c access, do the following:

a. Check the SNMPv2c Enabled checkbox.

b. In the SNMP Trap Community string field, enter the SNMP community string.

Step 5 Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files. You return to the All Devices table.

Related Topics

- Displaying Chassis Interfaces and Configuring High-Level Interface Attributes, page 4-34
- Displaying Modules by Chassis, page 4-68
- Managing Catalyst 6500 Series Chassis or Cisco 7600 Series Router VLANs, page 4-40

Configuring Catalyst 6500 Series Chassis, Catalyst 6500 Virtual Switching System 1440 Devices, and Cisco 7600 Series Routers Static Routes

You can configure static routes for the Catalyst 6500 Series Chassis, Catalyst 6500 Virtual Switching System 1440 Devices, and Cisco 7600 Series Routers. Though interfaces can be shared across contexts, the ACE supports only static routes for virtual contexts. You can configure static routes for Catalyst 6500 series chassis, Catalyst 6500 Virtual Switching System (VSS) 1440 devices, and Cisco 7600 series routers.

Note After a device static route has been created, you can modify only its administrative distance.

Procedure

Step 1 Choose **Config > Devices > All Devices**.

The device tree appears.

Step 2 In the device tree, choose the device that you want to configure, and choose **Network > Static Routes**.

The Static Routes table appears.

Step 3 In the Static Routes table, click **Add** to configure a new static route for the device, or choose an existing static route, and click **Edit** to modify it.

The Static Routes configuration window appears.

Step 4 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.

Step 5 In the Destination Prefix Mask field, choose the subnet for the static route.

Step 6 In the Next Hop field, enter the IP address of the gateway router for the route.

The gateway address must be on the same network as a VLAN interface for the device.

Step 7 In the Admin Distance field, enter the administrative distance value of the route.

The administrative distance is the first criterion that a router uses to determine which routing protocol to use if two protocols provide route information for the same destination. The administrative distance is a measure of the trustworthiness of the source of the routing information.

A lower administrative distance value indicates that the protocol is more reliable. Valid entries are from 0 to 255, with lower numbers indicating greater reliability. For example, a static route has an administrative distance value of 1 while an unknown protocol has an administrative distance value of 255.

Table 4-10 lists default distance values of the protocols that Cisco supports.

Table 4-10 Cisco Default Distance Value Table

Route Source	Administrative Distance Value
Connected interface	0
Static route	1
Enhanced Interior Gateway Routing Protocol (EIGRP) summary route	5
External Border Gateway Protocol (BGP)	20
Internal EIGRP	90
IGRP	100
OSPF (Open Shortest Path First)	110
Intermediate System-to-Intermediate System (IS-IS)	115
Routing Information Protocol (RIP)	120
Exterior Gateway Protocol (EGP)	140
On-Demand Routing (ODR)	160
External EIGRP	170
Internal BGP	200
Unknown	255

Step 8 Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files. You return to the Static Route table.
- Click **Cancel** to exit the procedure without saving your entries and to return to the Static Route table.
- Click **Next** to deploy your entries and to add another static route.

Related Topics

- Managing Catalyst 6500 Series Chassis or Cisco 7600 Series Router VLANs, page 4-40
- Displaying All Device VLANs, page 4-41

- Adding and Managing Devices, page 4-1

Configuring Catalyst 6500 Series Chassis or Cisco 7600 Series Router Interfaces

This section shows how to configure the interface attributes for the Catalyst 6500 series chassis or Cisco 7600 series router.

This section includes the following topics:

- Displaying Chassis Interfaces and Configuring High-Level Interface Attributes
- Configuring Access Ports
- Configuring Trunk Ports
- Configuring Switch Virtual Interfaces
- Configuring Routed Ports

Displaying Chassis Interfaces and Configuring High-Level Interface Attributes

You can display a complete list of interfaces on a selected Catalyst 6500 series chassis or Cisco 7600 series router. From this display, you can configure the following high-level attributes for a specified interface: interface description, operating mode, and administrative state.

Procedure

Step 1 Choose **Config > Devices > All Devices**.

The device tree appears.

Step 2 In the device tree, choose the device, and choose **Interfaces > Summary**.

The Interfaces table appears, listing all interfaces on the device and related information as follows:

- Interface name
- Description, if available
- Configured state, such as Up or Down
- Current operational state, if known
- Mode of operation, such as Access, Routed, or Trunk
- Interface hardware type

Step 3 Choose the interface to configure, and click **Edit**.

The configuration window appears.

Step 4 Enter the following:

a. In the Description field, enter a brief description of the interface.

b. In the Administrative State field, choose **Up** or **Down** to indicate whether the port should be up or down.

c. In the Mode field, choose the operational mode of the interface: **Trunk**, **Access**, or **Routed**.

d. Click **Apply** to save your changes or **Cancel** to exit the procedure without saving your changes.

The Interfaces table appears.

Related Topics

- Configuring Access Ports, page 4-35
- Configuring Trunk Ports, page 4-36
- Configuring Routed Ports, page 4-39
- Configuring Switch Virtual Interfaces, page 4-38
- Creating VLAN Groups, page 4-44
- Managing Catalyst 6500 Series Chassis or Cisco 7600 Series Router VLANs, page 4-40

Configuring Access Ports

You can configure access port attributes for a selected device. An access port receives and sends traffic in native formats with no VLAN tagging. Traffic that arrives on an access port is assumed to belong to the VLAN assigned to the port. If an access port receives a tagged packet (Inter-Switch Link [ISL] or 802.1Q tagged), the packet is dropped, and the source address is not learned.

Procedure

Step 1 Choose **Config > Devices > All Devices**.

The device tree appears.

Step 2 In the device tree, choose the device that you want to configure an access port for, and choose **Interfaces > Access Ports**.

The Interfaces table appears.

Step 3 From the Interfaces table, choose the port that you want to configure, and click **Edit**.

The Access Ports configuration window appears.

Step 4 In the Description field, enter a description for the port.

Valid entries are unquoted text strings with a maximum of 240 characters including spaces.

Step 5 In the Administrative State field, choose **Up** or **Down** to indicate whether the port should be up or down.

Step 6 In the Speed field, either specify the speed at which the interface is to operate or that the interface is to automatically negotiate its speed:

- **Auto**—The interface is to automatically negotiate speed with the connected device.
- **10 Mbps**—The interface is to operate at 10 Mbps.
- **100 Mbps**—The interface is to operate at 100 Mbps.
- **1000 Mbps**—The interface is to operate at 1000 Mbps.

Step 7 In the Duplex Mode field, specify whether the interface is to automatically negotiate its duplex mode or use full- or half-duplex mode:

- **Auto**—The interface is to automatically negotiate duplex mode with the connected device.
- **Full**—The interface is to operate in full-duplex mode. In this mode, two connected devices can send and receive traffic at the same time.

- **Half**—The interface is to operate in half-duplex mode. In this mode, two connected devices can either send or receive traffic.

Step 8 In the VLANs field, enter individual names for each VLAN to which the interface belongs.

The allowable range is 1 to 4094.

Step 9 Do one of the following:

- Click **Apply** to save your entries and to return to the Interfaces table.
- Click **Cancel** to exit the procedure without saving your entries and to return to the Interfaces table.

Related Topics

- Configuring Trunk Ports, page 4-36
- Configuring Switch Virtual Interfaces, page 4-38
- Configuring Routed Ports, page 4-39
- Managing Catalyst 6500 Series Chassis or Cisco 7600 Series Router VLANs, page 4-40

Configuring Trunk Ports

You can configure trunk ports for a selected device. A trunk port carries the traffic of multiple VLANs and by default is a member of all VLANs in the VLAN database. Two types of trunk ports are as follows:

- In an Inter-Switch Link (ISL) trunk port, all received packets are expected to be encapsulated with an ISL header, and all transmitted packets are sent with an ISL header. Native (nontagged) frames received from an ISL trunk port are dropped.
- An IEEE 802.1Q trunk port supports simultaneous tagged and untagged traffic. An 802.1Q trunk port is assigned a default port VLAN ID or *native VLAN*, and all untagged traffic travels on the native VLAN. All untagged traffic and tagged traffic with a NULL VLAN ID are assumed to belong to the native VLAN. A packet with a VLAN ID that is equal to the outgoing port native VLAN is sent untagged. All other traffic is sent with a VLAN tag.

Procedure

Step 1 Choose **Config > Devices > All Devices**.

The device tree appears.

Step 2 In the device tree, choose the device that you want to configure, and choose **Interfaces > Trunk Ports**.

The Interfaces table appears.

Step 3 In the Interfaces table, choose the port that you want to configure, and click **Edit**.

The Trunk Port configuration window appears.

Step 4 Configure the port using the information in Table 4-11.

Table 4-11 Trunk Port Configuration Attributes

Field	Description
Description	Description for the port. Valid entries are unquoted text strings with a maximum of 240 characters including spaces.
Administrative State	Up or Down to indicate whether the port should be up or down.
Speed	Speed at which the interface is to operate or that the interface is to automatically negotiate its speed: • **Auto**—The interface is to automatically negotiate speed with the connected device. • **10 Mbps**—The interface is to operate at 10 Mbps. • **100 Mbps**—The interface is to operate at 100 Mbps. • **1000 Mbps**—The interface is to operate at 1000 Mbps.
Duplex Mode	Whether the interface is to automatically negotiate its duplex mode or use full-duplex or half-duplex mode: • **Auto**—The interface is to automatically negotiate duplex mode with the connected device. • **Full**—The interface is to operate in full-duplex mode. In this mode, two connected devices can send and receive traffic at the same time. • **Half**—The interface is to operate in half-duplex mode. In this mode, two connected devices can either send or receive traffic.
Trunk Mode	How the interface is to interact with neighboring interfaces: • **Dynamic**—The interface is to convert a link to a trunk link if the neighboring interface is set to trunk or desirable mode. • **Dynamic Desirable**—The interface is to actively attempt to convert a link to a trunk link. The interface becomes a trunk interface if the neighboring interface is set to trunk, desirable, or auto mode. • **Static**—The interface is to enter permanent trunking mode and to negotiate converting a link into a trunk link. The interface becomes a trunk interface even if the neighboring interface does not change.
Desired Encapsulation	Type of encapsulation to be used on the trunk port: • **Dot1Q**—The interface is to use 802.1Q encapsulation. • **Negotiate**—The interface is to negotiate with the neighboring interface to use ISL (Inter-Switch Link) (preferred) or 802.1Q encapsulation, depending on the configuration and capabilities of the neighboring interface. • **ISL**—The interface is to use ISL encapsulation.
Native VLAN	VLAN to use as the native VLAN for the trunk in 802.1Q trunking mode. VLAN 1 (1) is the default native VLAN.
VLANs	VLANs to which the interface belongs (allowable range is 1-4094). You can also enter ranges of VLANs, such as 101-120, 130.
Prune VLANs	VLANs that can be pruned (allowable range is 1-4094). VTP pruning blocks unneeded flooded traffic to VLANs on trunk ports that are included in this field. Only VLANs included in this field can be pruned. You can also specify ranges of VLANs that can be pruned, such as 75, 121-250, 351.

Step 5 Do one of the following:

- Click **Apply** to save your entries and to return to the Interfaces table.
- Click **Cancel** to exit the procedure without saving your entries and to return to the Interfaces table.

Related Topics

- Configuring Access Ports, page 4-35
- Configuring Switch Virtual Interfaces, page 4-38
- Configuring Routed Ports, page 4-39
- Managing Catalyst 6500 Series Chassis or Cisco 7600 Series Router VLANs, page 4-40

Configuring Switch Virtual Interfaces

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

Procedure

Step 1 Choose **Config > Devices > All Devices**.

The device tree appears.

Step 2 In the device tree, choose the device that you want to configure, and choose **Interfaces > Switched Virtual Interfaces**.

The Interfaces table appears.

Step 3 In the Interfaces table, click **Add** to add a new SVI, or choose the interface you want to configure, and click **Edit**.

The Switched Virtual Interfaces configuration window appears.

Step 4 In the VLANs field, specify the VLAN to use in one of the following ways:

- To specify a new VLAN, choose the first radio button, and then enter a new VLAN.
- To choose an existing VLAN, choose the second radio button, and choose one of the existing VLANs.

Note You cannot modify a VLAN for an existing SVI.

Step 5 In the Description field, enter a description for the SVI. Valid entries are unquoted text strings with a maximum of 240 characters including spaces.

Step 6 In the Administrative State field, choose **Up** or **Down** to indicate whether the SVI should be up or down.

Step 7 In the IP Address field, enter the IP address to be used for the interface on the MSFC in dotted-decimal format.

Step 8 In the Netmask field, choose the subnet mask to be used for the IP address.

Step 9 Do one of the following:

- Click **Apply** to save your entries and to return to the Interfaces table.
- Click **Cancel** to exit the procedure without saving your entries and to return to the Interfaces table.

Related Topics

- Configuring Access Ports, page 4-35
- Configuring Trunk Ports, page 4-36
- Configuring Routed Ports, page 4-39
- Managing Catalyst 6500 Series Chassis or Cisco 7600 Series Router VLANs, page 4-40

Configuring Routed Ports

You can configure routed ports on a specified device. A routed port is a physical port that acts like a port on a router; however, it does not have to be connected to a router. A routed port is not associated with a particular VLAN, as is an access port. A routed port behaves like a regular router interface, except that it does not support VLAN subinterfaces. Routed ports can be configured with a Layer 3 routing protocol. A routed port is a Layer 3 interface only and does not support Layer 2 protocols, such as Dynamic Trunking Protocol (DTP) and Spanning Tree Protocol (STP).

Procedure

Step 1 Choose **Config > Devices > All Devices**.

The device tree appears.

Step 2 In the device tree, choose the device that you want to configure, and choose **Interfaces > Routed Ports**.

The Interfaces table appears.

Step 3 In the Interfaces table, choose the interface that you want to configure, and click **Edit**.

The Routed Ports configuration window appears.

Step 4 In the Description field, enter a description for the interface. Valid entries are unquoted text strings with a maximum of 240 characters including spaces.

Step 5 In the Administrative State field, choose **Up** or **Down** to indicate whether the interface should be up or down.

Step 6 In the Speed field, either specify the speed at which the interface is to operate or that the interface is to automatically negotiate its speed:

- **Auto**—The interface is to automatically negotiate speed with the connected device.
- **10 Mbps**—The interface is to operate at 10 Mbps.
- **100 Mbps**—The interface is to operate at 100 Mbps.
- **1000 Mbps**—The interface is to operate at 1000 Mbps.

Step 7 In the Duplex Mode field, specify whether the interface is to automatically negotiate its duplex mode, or use full- or half-duplex mode:

- **Auto**—The interface is to automatically negotiate duplex mode with the connected device.
- **Full**—The interface is to operate in full-duplex mode. In this mode, two connected devices can send and receive traffic at the same time.

- **Half**—The interface is to operate in half-duplex mode. In this mode, two connected devices can either send or receive traffic.

Step 8 In the IP Address field, enter the IP address to be used for the interface in dotted-decimal format.

Step 9 In the Netmask field, choose the subnet mask to be used for the IP address.

Step 10 Do one of the following:

- Click **Apply** to apply your entries and to return to the Interfaces table.
- Click **Cancel** to exit the procedure without saving your entries and to return to the Interfaces table.

Related Topics

- Configuring Trunk Ports, page 4-36
- Configuring Switch Virtual Interfaces, page 4-38
- Configuring Access Ports, page 4-35
- Managing Catalyst 6500 Series Chassis or Cisco 7600 Series Router VLANs, page 4-40

Managing Catalyst 6500 Series Chassis or Cisco 7600 Series Router VLANs

You can add a VLANs and VLAN groups to a Catalyst 6500 series chassis or Cisco 7600 series router that you use when configuring the interfaces for an installed ACE module, which does not have any external physical interfaces. Instead, the ACE module uses internal VLAN interfaces. For information about configuring VLANs for use with virtual contexts, see the "Configuring VLAN Interfaces" section on page 11-5. For more information about VLANs and their use with ACE modules, see the *Cisco Application Control Engine Module Routing and Bridging Configuration Guide*.

This section contains the following topics:

- Adding Device VLANs, page 4-40
- Displaying All Device VLANs, page 4-41
- Configuring Device Layer 3 VLANs, page 4-43
- Configuring Device Layer 2 VLANs, page 4-42
- Displaying All Device VLANs, page 4-41
- Creating VLAN Groups, page 4-44

Adding Device VLANs

You can add a VLAN to a Catalyst 6500 series chassis or Cisco 7600 series router.

Procedure

Step 1 Choose **Config > Devices > All Devices**.

The device tree appears.

Step 2 In the device tree, choose the device that you want to configure, and choose **VLANs > Layer 2** or **VLANs > Layer 3**.

The VLANs table appears.

Step 3 From the VLANs table, click **Add**.

The VLAN configuration window appears.

Step 4 Configure the VLAN using the information in Table 4-12.

Table 4-12 Device VLAN Configuration Attributes

Field	Description
VLAN	Unique identifier for the VLAN. Valid entries are from 1 to 4094.
Name	Name for the VLAN.
Description	Description for the VLAN. Valid entries are unquoted text strings with a maximum of 240 characters including spaces.
Access Ports	Access ports. From the Available Items list, click **Add**.To remove a port that you do not want to use, choose the port from the Selected Items list, and click **Remove**.
Trunk Ports	Trunk ports. From the Available Items list, click **Add**.To remove a port that you do not want to use, choose the port from the Selected Items list, and click **Remove**.
VTP Domain	Name of the VTP domain to which the VLAN belongs. A VTP domain is made up of one or more interconnected network devices that share the same VTP domain name. A network device can be configured to be in one and only one VTP domain.
IP Address	Field that appears for Layer 3 VLANs only. Enter the IP address to be used for the VLAN interface. Enter the IP address in dotted-decimal notation, such as 192.168.1.1.
Mask	Field that appears for Layer 3 VLANs only. Choose the subnet mask to apply to the IP address.

Step 5 Do one of the following:

- Click **Apply** to apply your entries and to return to the VLAN Management table.
- Click **Cancel** to exit the procedure without saving your entries and to return to the VLAN Management table.

Related Topics

- Managing Catalyst 6500 Series Chassis or Cisco 7600 Series Router VLANs, page 4-40
- Configuring Device Layer 2 VLANs, page 4-42
- Configuring Device Layer 3 VLANs, page 4-43
- Displaying All Device VLANs, page 4-41
- Creating VLAN Groups, page 4-44

Displaying All Device VLANs

You can display all configured VLANs on a Catalyst 6500 series chassis or Cisco 7600 series router.

Procedure

Step 1 Choose **Config > Devices > All Devices**.

The device tree appears.

Step 2 In the device tree, choose the device with VLANs that you want to display, and choose **VLANs > Summary**.

The VLANs table appears, listing all VLANs on the selected chassis and related information:

- VLAN number
- Name given to the VLAN
- VLAN type, such as Layer 2 or Layer 3
- Number of access ports
- Number of trunk ports
- VLAN Trunking Protocol (VTP) domain to which the VLAN belongs

Related Topics

- Managing Catalyst 6500 Series Chassis or Cisco 7600 Series Router VLANs, page 4-40
- Configuring Device Layer 2 VLANs, page 4-42
- Configuring Device Layer 3 VLANs, page 4-43
- Displaying All Device VLANs, page 4-41
- Creating VLAN Groups, page 4-44

Configuring Device Layer 2 VLANs

You can add or modify a Layer 2 VLAN on a Catalyst 6500 series chassis or Cisco 7600 series router.

Procedure

Step 1 Choose **Config > Devices > All Devices**.

The device tree appears.

Step 2 In the device tree, choose the device that you want to configure a Layer 2 VLAN for, and choose **VLANs > Layer 2**.

The VLANs table appears, listing all Layer 2 VLANs associated with the chassis.

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

The VLAN configuration window appears.

Step 4 Configure the VLAN using the information in Table 4-12.

Step 5 Do one of the following:

- Click **Apply** to apply your entries and to return to the VLAN Management table.

- Click **Cancel** to exit the procedure without saving your entries and to return to the VLAN Management table.

Related Topics

- Managing Catalyst 6500 Series Chassis or Cisco 7600 Series Router VLANs, page 4-40
- Adding Device VLANs, page 4-40
- Configuring Device Layer 3 VLANs, page 4-43
- Displaying All Device VLANs, page 4-41
- Creating VLAN Groups, page 4-44

Configuring Device Layer 3 VLANs

You can add or modify a Layer 3 VLAN on a Catalyst 6500 series chassis or Cisco 7600 series router.

Procedure

Step 1 Choose **Config > Devices > All Devices**.

The device tree appears.

Step 2 In the device tree, choose the device that you want to configure a Layer 3 VLAN for, and choose **VLANs > Layer 3**.

The VLANs table appears, listing all Layer 3 VLANs associated with the chassis.

Step 3 In the VLANs table, click **Add** to add a new VLAN, or choose an existing VLAN, and click **Edit** to modify it.

The VLAN configuration window appears.

Step 4 Configure the VLAN using the information in Table 4-12.

Step 5 Do one of the following:

- Click **Apply** to apply your entries and to return to the VLAN Management table.
- Click **Cancel** to exit the procedure without saving your entries and to return to the VLAN Management table.

Related Topics

- Managing Catalyst 6500 Series Chassis or Cisco 7600 Series Router VLANs, page 4-40
- Information About Virtual Contexts, page 5-2

Modifying Device VLANs

You can modify VLANs for a specific device.

Procedure

Step 1 Choose **Config > Devices > All Devices**.

The device tree appears.

Step 2 In the device tree, choose the device with the VLAN that you want to modify, and choose **VLANs > Layer 2** or **VLANs > Layer 3**.

The VLANs table appears.

Step 3 Choose the VLAN you want to modify, and then click **Edit**.

The VLAN configuration window appears.

Step 4 Modify the VLAN configuration using the information in Table 4-12.

Step 5 Do one of the following:

- Click **Apply** to save your entries and to return to the VLANs table.
- Click **Cancel** to exit the procedure without saving your entries and to return to the VLANs table.

Related Topics

- Managing Catalyst 6500 Series Chassis or Cisco 7600 Series Router VLANs, page 4-40
- Displaying All Device VLANs, page 4-41
- Adding Device VLANs, page 4-40
- Creating VLAN Groups, page 4-44

Creating VLAN Groups

You can create VLAN groups on a Catalyst 6500 series chassis or Cisco 7600 series router and assign each group an ACE module. For an ACE module to receive traffic from the Catalyst supervisor module and VSS devices, you must create VLAN groups on the supervisor module, and then assign the groups to the ACE module. When the VLANs are configured on the supervisor module to the ACE module, you can configure the VLANs on the ACE module.

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

Procedure

Step 1 Choose **Config > Devices > All Devices**.

The device tree appears.

Step 2 In the device tree, choose the device that you want to create a VLAN group for, and choose **VLANs > Groups**.

The Groups table appears.

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

The Groups configuration window appears.

Step 4 In the VLAN Group Id field, enter a unique numerical identifier for the VLAN group.

Valid entries are unquoted number strings with any value between 1-65535. Available Module Slot numbers will appear underneath this field.

Step 5 In the Module Slot Numbers field, select the ACE module(s) that you want to associate with the VLAN group.

Step 6 Double click or the number, or single click the arrow to the right of the Available Modules field for the slot numbers to the Selected field.

Step 7 In the VLANs field, enter the VLANs to be included in the VLAN group. Valid entries are individual names for each VLAN or ranges of VLANs (allowable range is 1-4094), such as 10, 50-110.

Step 8 Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files. You return to the Groups table.
- Click **Cancel** to exit the procedure without saving your entries and to return to the Groups table.
- Click **Next** to deploy your entries and to add another VLAN group.

Related Topics

- Managing Catalyst 6500 Series Chassis or Cisco 7600 Series Router VLANs, page 4-40
- Configuring Device Layer 3 VLANs, page 4-43
- Configuring Device Layer 2 VLANs, page 4-42
- Displaying All Device VLANs, page 4-41

Configuring ACE Module and Appliance Role-Based Access Controls

ANM provides an interface to allow you to configure device Role-Based Access Control (RBAC) on the device only. The RBAC feature applies to ACE modules and appliances only and is applicable only on the device and is not enforced by ANM. If you want to set up authorization in ANM, go to **Admin > Role-Based Access Control**.

This section includes the following topics:

- Configuring Device RBAC Users, page 4-45
- Configuring Device RBAC Roles, page 4-49
- Configuring Device RBAC Domains, page 4-53

Configuring Device RBAC Users

ANM provides an interface that allows you to configure user access to your device through role-based access controls on the device only. This configuration is applicable only on the device and will not be enforced by ANM.

Use the Role-Based Access Control feature to specify the people that are allowed to log onto a device.

This section includes the following topics:

- Guidelines for Managing Users, page 4-46
- Displaying a List of Device Users, page 4-46
- Configuring Device User Accounts, page 4-46

- Modifying Device User Accounts, page 4-47
- Deleting Device User Accounts, page 4-48

Guidelines for Managing Users

Follow these guidelines for managing users:

- For users that you create in the Admin context, the default scope of access is for the entire ACE.
- If you do not assign a role to a new user, the default user role is Network-Monitor. For users that you create in other contexts, the default scope of access is the entire context.
- Users cannot log in until they are associated with a domain and a user role.
- You cannot delete roles and domains that are associated with an existing user.

Related Topics

- Configuring Device RBAC Users, page 4-45
- Configuring ACE Module and Appliance Role-Based Access Controls, page 4-45

Displaying a List of Device Users

You can display of list of users that can access an ACE context.

Procedure

Step 1 Choose **Config > Devices >** *context* **> Role-Based Access Control > Users**.

The Users table appears with the following fields:

- User Name
- Expiry Date
- Role
- Domains

Step 2 (Optional) You can use the options in this window to create a new user or modify or delete any existing user to which you have access (see Table 4-13).

Related Topics

- Configuring Device RBAC Users, page 4-45
- Configuring ACE Module and Appliance Role-Based Access Controls, page 4-45

Configuring Device User Accounts

You can add or modify a user account in a selected ACE context.

Note This configuration is applicable only on the device or building block and is not enforced by ANM. To manipulate ANM RBAC, go to Admin > Role-Based Access Control.

Procedure

Step 1 Choose the item to configure:

- To configure a virtual context, choose **Config > Devices >** *context* **> Device RBAC > Users**.
- To configure a configuration building block, choose **Config > Global > Building Blocks >** *building_block* **> Role-Based Access Control > Users**.

A list of users appears.

Step 2 In the Users table, click **Add** to add a new user, or choose the user that you want to configure and click **Edit**.

The Users configuration window appears.

Step 3 Configure the user attributes using the information in Table 4-13.

Table 4-13 User Attributes

Field	Description
User Name	Name by which the user is to be identified (up to 24 characters). Only letters, numbers, and an underscore can be used. The field is case sensitive.
Expiry Date	Date that user account expires (optional).
Password Entered As	Password for this user account. You can choose Clear Text or Encrypted Text.
Password	Password for the user account.
Confirm Password	Password for this account that you reenter.
Encryption	Password in either clear or encrypted text.
Role	Role that you customize or accept as an existing role. To enter the Role for this user, see the "Configuring Device User Roles" section on page 4-50. See Table 4-14 for details about setting up new roles.
Domains	Domains to which this user belongs. Use the **Add** and **Remove** buttons.

Step 4 Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.

The Users table appears.

Related Topics

- Configuring Device RBAC Users, page 4-45
- Configuring ACE Module and Appliance Role-Based Access Controls, page 4-45

Modifying Device User Accounts

You can modify an existing user account in a selected ACE context.

Note This configuration is applicable only on the device or building block and will not be enforced by ANM. To manipulate ANM RBAC, go to Admin > Role-Based Access Control.

Procedure

Step 1 Choose the item to configure:

- To configure a virtual context, choose **Config > Devices >** *context* **> Device RBAC > Users**.
- To configure a configuration building block, choose **Config > Global > Building Blocks >** *building_block* **> Role-Based Access Control > Users**.

A table of users, expiration dates, roles, and domains appears.

Step 2 Choose the user account that you want to modify.

Step 3 Click **Edit**.

Step 4 Modify any of the attributes in the table (see Table 4-13).

Step 5 Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.

The Users table appears.

Related Topics

- Configuring Device RBAC Users, page 4-45
- Configuring ACE Module and Appliance Role-Based Access Controls, page 4-45

Deleting Device User Accounts

You can delete an existing device RBAC user account in a selected ACE context.

Note This configuration is applicable only on the device or building block and will not be enforced by ANM. To manipulate ANM RBAC, go to Admin > Role-Based Access Control.

Procedure

Step 1 Choose the item to configure:

- To configure a virtual context, choose **Config > Devices >** *context* **> Device RBAC > Users**.
- To configure a configuration building block, choose **Config > Global > Building Blocks >** *building_block* **> Role-Based Access Control > Users**.

A table of users, roles, and domains appears.

Step 2 In the table, choose the user account to delete, and click **Delete**.

A confirmation window appears.

Step 3 In the confirmation window, do one of the following:

- Click **OK** to remove the user account from the ANM database and return to the Users table.
- Click **Cancel** to return to the Users table without deleting the user account.

Related Topics

- Configuring Device RBAC Users, page 4-45
- Configuring ACE Module and Appliance Role-Based Access Controls, page 4-45

Configuring Device RBAC Roles

This section shows how to configure RBAC roles and includes the following topics:

- Guidelines for Managing User Roles, page 4-49
- Role Mapping in Device RBAC, page 4-49
- Configuring Device User Roles, page 4-50
- Modifying Device User Roles, page 4-52
- Deleting Device User Roles, page 4-52

Guidelines for Managing User Roles

Follow these guidelines to manage user roles:

- Administrators can view and modify all roles.
- Other users can view only the roles assigned to them.
- You cannot change the default roles.
- Role permissions are different based on whether they were created in either an Admin context or in a user context. If you want to allow users to switch between contexts, ensure that they have a predefined role. If you want to restrict a user to only their home context, assign them a customized user role.
- Certain role features are available only to default roles, for example, an Admin role in the Admin context would have **changeto** and **system** permissions to perform tasks such as license management, resource class management, HA setup, and so on. User-created roles cannot use these features.

Related Topics

- Role Mapping in Device RBAC, page 4-49
- Controlling Access to Cisco ANM, page 17-3
- Configuring Device RBAC Users, page 4-45
- Configuring Device RBAC Roles, page 4-49
- Configuring Device RBAC Domains, page 4-53
- How ANM Handles Role-Based Access Control, page 17-8

Role Mapping in Device RBAC

When you are logged into a specific device RBAC, you see the tasks that you have been given permission to access. Features and menus that are not applicable for your role will not display.

Since the predefined roles encompass all the role types you may need, we encourage you to use them. If you choose to define your own roles, be aware that rules features are not a one-to-one mapping from a CLI feature to ANM menu task.

Defining the proper rules for your user-defined role will require you to create a mapping between the features in Device RBAC and the ANM menu tasks. For example, in order to manage virtual servers, you must choose the following six menu features (Real Servers, Server Farms, VIP, Probes, Loadbalance, NAT, and Interface) in your role.

Note Certain features in ANM do not have a corresponding feature mapping on the CLI. For example, class maps and SNMP do not have a corresponding feature mapping. To modify these features, you need to choose a predefined role that a contains at least one feature with the Modify permission on it.

Related Topics

- How ANM Handles Role-Based Access Control, page 17-8
- Understanding Roles, page 17-6

Configuring Device User Roles

You can edit the predefined roles, or you can create or edit user-defined roles. When you create a new role, you specify a name and description of the new role, and then choose the operations privileges for each task. You can also assign this role to one or more users.

Note This configuration is applicable only on the device or building block and will not be enforced by the ANM. To manipulate the ANM RBAC, go to Admin > Role-Based Access Control.

Procedure

Step 1 Choose the item to configure:

- To configure a virtual context, choose **Config > Devices >** *context* **> Device RBAC > Roles**.
- To configure a configuration building block, choose **Config > Global > Building Blocks >** *building_block* **> Role-Based Access Control > Roles**.

A table of the defined roles and their settings appears.

Step 2 In the table, choose the type of configuration that you want to perform as follows:

- To add a new role, click **Add**, enter the following attributes, and then click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.

Table 4-14 Role Attributes

Attribute	Description
Name	Name of the role.
Description	Brief description of the role.

- To edit an existing role, choose the role, and click **Edit**.

  The Roles configuration window appears.

Step 3 Click **Edit.**

The Rule table appears.

Step 4 In the Rule table, click **Add** to create rules for this role, or choose the rule that you want to configure, and click **Edit**.

See Table 4-15 for rule attribute descriptions.

Table 4-15 Rule Attributes

Attribute	Description
Rule Number	Number assigned to this rule.
Permission	Permit or deny the specified operation.
Operation	Create, debug, modify[1], and monitor the specified feature.
Feature	AAA, Access List, Change To Context, Config Copy, Connection, DHCP, Exec-Commands, Fault Tolerant, Inspect, Interface, Load Balance, NAT, PKI, Probe, Real Inservice, Routing, Real Server, Server Farm, SSL[2], Sticky, Syslog, and VIP. The Changeto feature allows you to move from the Admin context to another virtual context and maintain the same role with the same privileges in the new context that you had in the Admin context. This feature applies only to the Admin context and to the following ACE software versions: • ACE module software version A2(1.3) and later releases. • ACE appliance software version A3(2.2) and later releases. The Exec-commands feature enables all default custom role commands in the ACE. The default custom role commands are capture, debug, gunzip, mkdir, move, rmkdir, tac-pac, untar, write, and undebug. This feature applies to both Admin and user contexts and to the following ACE software versions: • ACE module software version A2(1.3) and later releases. • ACE appliance software version A3(2.2) and later releases.

1. Certain features are not available for certain operations. For modify, the following features cannot be used: Changeto, config-copy, DHCP, Exec-commands, NAT, real-inservice, routing, and syslog.
2. For all SSL-related operations, a user with a custom role should include the following two rules: A rule that includes the SSL feature, and a rule that includes the PKI feature.

Step 5 Click **Deploy Now** to update the rule for this role or click **Next** to deploy this rule and move to another rule.

Step 6 Click **Deploy Now** to update this role and save this configuration to the running-configuration and startup-configuration files.

Related Topics

- Configuring Device RBAC Roles, page 4-49
- Configuring ACE Module and Appliance Role-Based Access Controls, page 4-45

Modifying Device User Roles

You can modify any user-defined role.

Note This configuration is applicable only on the device or building block and will not be enforced by ANM. To manipulate ANM RBAC, go to Admin > Role-Based Access Control.

Procedure

Step 1 Choose the item to configure:

- To configure a virtual context, choose **Config > Devices >** *context* **> Device RBAC > Roles**.
- To configure a configuration building block, choose **Config > Global > Building Blocks >** *building_block* **> Role-Based Access Control > Roles**.

A table of the defined roles and their settings appears.

Step 2 In the table, choose the role that you want to modify.

Step 3 Click **Edit**. For details on updating role rules, see Table 4-15.

Step 4 Make the changes.

For details on updating role rules, see the "Adding, Editing, or Deleting Rules" section on page 4-53.

Step 5 Click **Deploy Now** to update the rules for this role and save this configuration to the running-configuration and startup-configuration files.

Related Topics

- Configuring Device RBAC Roles, page 4-49
- Configuring ACE Module and Appliance Role-Based Access Controls, page 4-45

Deleting Device User Roles

You can delete any user-defined roles.

Note This configuration is applicable only on the device or building block and will not be enforced by ANM. To manipulate ANM RBAC, go to Admin > Role-Based Access Control.

Procedure

Step 1 Choose the item to configure:

- To configure a virtual context, choose **Config > Devices >** *context* **> Device RBAC > Roles**.
- To configure a configuration building block, choose **Config > Global > Building Blocks >** *building_block* **> Role-Based Access Control > Roles**.

The Roles table appears.

Step 2 In the Roles table, choose the role to delete, and click **Delete**.

Step 3 Click **OK** to confirm the deletion.

Users that have the deleted role no longer have that access.

Related Topics

- Configuring Device RBAC Roles, page 4-49
- Configuring ACE Module and Appliance Role-Based Access Controls, page 4-45

Adding, Editing, or Deleting Rules

You can change or delete rules to redefine what feature access a specific role contains.

Note This configuration is applicable only on the device or building block and will not be enforced by ANM. To manipulate ANM RBAC, go to Admin > Role-Based Access Control.

Procedure

Step 1 After selecting the user-defined role, click **Edit**.

The Rule window appears.

Step 2 Do one of the following:

- To create a new rule, click **Add**. Enter the rule information (see Table 4-15 on page 4-51), and then click **Deploy Now** to add the rule or **Next** to deploy this rule and add another rule.
- To change an existing rule, choose a rule and click **Edit**. Click **Deploy Now** to save this rule to the running-configuration and startup-configuration files.
- To remove rules from a role, choose the rules to remove, and click **Delete**. Click **OK** to confirm its deletion.

Step 3 Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.

Related Topics

- Configuring Device RBAC Roles, page 4-49
- Configuring ACE Module and Appliance Role-Based Access Controls, page 4-45

Configuring Device RBAC Domains

You can configure device RBAC domains.

This section includes the following topics:

- Guidelines for Managing Domains, page 4-54
- Displaying Domains for a Device, page 4-54
- Configuring Device Domains, page 4-55
- Modifying Device Domains, page 4-57

- Deleting Device Domains, page 4-57

Related Topics

- Information About Device Management, page 4-2
- How ANM Handles Role-Based Access Control, page 17-8
- Configuring ACE Module and Appliance Role-Based Access Controls, page 4-45

Guidelines for Managing Domains

Follow these guidelines for managing domains:

- Devices and their components must already be configured in order for them to be added to a domain.
- Domains are *logical* concepts. You do *not* delete a member of a domain when you delete the domain.
- The predefined default domain cannot be modified or deleted.
- Normally, a user is associated with the default domain, which allows the user to see all configurations within the context. When a user is configured with a customized domain, then the user can see only what is in the domain.

Related Topics

- Configuring Device RBAC Domains, page 4-53
- Configuring ACE Module and Appliance Role-Based Access Controls, page 4-45

Displaying Domains for a Device

You can display domains for a device.

Note Your user role determines whether you can use this option.

Procedure

Step 1 Choose the item to view:

- To view a domain for the device's virtual context, choose **Config > Devices >** *context* **> Device RBAC > Domains**.
- To view a domain for a a configuration building block, choose **Config > Global > Building Blocks >** *building block* **> Role-Based Access Control > Domains**.

The Domains table appears.

Step 2 Expand the Domains table until you can see all the network domains.

Step 3 Choose a domain to display the settings for that domain.

You can also perform these tasks from this window:

- Configuring Device Domains, page 4-55
- Modifying Device Domains, page 4-57
- Deleting Device Domains, page 4-57

Related Topics

- Configuring Device RBAC Domains, page 4-53
- Configuring ACE Module and Appliance Role-Based Access Controls, page 4-45

Configuring Device Domains

You can add or modify domains on a selected device, such as a Catalyst 6500 series chassis.

Note This configuration is applicable only on the device or building block and will not be enforced by ANM. To manipulate ANM RBAC, go to Admin > Role-Based Access Control.

Procedure

Step 1 Choose the item to configure:

- To configure a virtual context, choose **Config > Devices >** *context* **> Device RBAC > Domains**.
- To configure a configuration building block, choose **Config > Global > Building Blocks >** *building_block* **> Role-Based Access Control > Domains**.

The Domains table appears.

Step 2 In the Domains table, choose the type of configuration that you want to perform:

- To add a new domain, click **Add**, enter the Domain Name, and then click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.
- To edit a domain, choose the domain that you want to configure, and then click **Edit**.

The Domain Object field appears below the Domain Name in the content area.

Step 3 Click **Edit** to enter the Domain Object table.

Step 4 In the Domain Object table, choose the type of configuration that you want to perform:

- Click **Add** to create domain objects for this domain. See Table 4-16 for Domain Object attributes.
- To remove an object, choose the object that you want to remove, and then click **Delete**.

Table 4-16 Domain Attributes

Field	Description
Name	Field that appears when any specific object type is selected. Name of an existing object defined.
All Objects	Collection of objects in this domain. The following options may be available depending on your virtual context: • All • Access List EtherType • Access List Extended • Class Map • Interface VLAN • Interface BVI • Parameter Map • Policy Map • Probe • Real Server • Script • Server Farm • Sticky

Step 5 Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.

The Domains Edit window updates and displays the total object number next to the object name.

Related Topics

- Configuring Device RBAC Domains, page 4-53
- Configuring ACE Module and Appliance Role-Based Access Controls, page 4-45

Modifying Device Domains

You can change the settings in a domain.

Note This configuration is applicable only on the device or building block and will not be enforced by ANM. To manipulate ANM RBAC, go to Admin > Role-Based Access Control.

Procedure

Step 1 Choose the item to configure:

- To configure a virtual context, choose **Config > Devices >** *context* **> Device RBAC > Domains**.
- To configure a configuration building block, choose **Config > Global > Building Blocks >** *building_block* **> Role-Based Access Control > Domains**.

Step 2 Choose the domain that you want to edit.

Step 3 Click **Edit**.

The Edit Domain window appears.

Step 4 Edit the object fields (see Table 4-16).

Step 5 Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.

Related Topics

- Configuring Device RBAC Domains, page 4-53
- Configuring ACE Module and Appliance Role-Based Access Controls, page 4-45

Deleting Device Domains

You can delete a network domain from ANM, and all the devices and subdomains that it contains.

Note This configuration is applicable only on the device or building block and will not be enforced by ANM. To manipulate ANM RBAC, go to Admin > Role-Based Access Control.

Procedure

Step 1 Choose the item to configure:

- To configure a virtual context, choose **Config > Devices >** *context* **> Device RBAC > Domains**.
- To configure a configuration building block, choose **Config > Global > Building Blocks >** *building_block* **> Role-Based Access Control > Domains**.

The Domains table appears.

Step 2 In the Domains table, choose the domain that you want to delete.

Step 3 Click **Delete**.

A prompt asks you to confirm this action.

Step 4 Click **OK**.

The domain is removed from the ANM database.

Related Topics

- Configuring Device RBAC Domains, page 4-53
- Configuring ACE Module and Appliance Role-Based Access Controls, page 4-45

Managing Devices

This section describes how to manage devices.

This section includes the following topics:

- Synchronizing Device Configurations, page 4-58
- Configuring User-Defined Groups, page 4-60
- Updating Device Passwords, page 4-64
- Changing ACE Module Passwords, page 4-65
- Restarting Device Polling, page 4-66
- Displaying All Devices, page 4-67
- Displaying Modules by Chassis, page 4-68
- Removing Modules from the ANM Database, page 4-69

Synchronizing Device Configurations

ANM provides three levels of synchronization. You can choose to synchronize from the device to ANM as follows:

- From the chassis level—Use this level when you want to synchronize Catalyst 6500 series chassis and module updates. See the "Synchronizing Chassis Configurations" section on page 4-59.
- From the ACE module level—Use this level when you want to synchronize changes to your ACE or CSM modules, such as new virtual contexts. See the "Synchronizing Module Configurations" section on page 4-59.
- From the virtual context level —Use this level in the Admin context to synchronize all current and new virtual contexts or at the user context level to synchronize a specific user context. See the "Synchronizing Virtual Context Configurations" section on page 5-91.

Caution If you see a difference in device information between what ANM displays and what you see by directly accessing the device through the CLI, ANM displays the data that is the least accurate. This condition can occur when the device is modified outside of ANM by using the CLI. We recommend that you synchronize the network devices up to the ANM using the synchronization option, which makes the ANM data more accurate.

Synchronizing Chassis Configurations

You can manually synchronize the configuration for Catalyst 6500 series switches, CSS devices, GSS devices and ACE appliances when there have been changes to a device that are not tracked in ANM.

Note ANM does not support auto synchronization for the Catalyst 6500 series switches, Cisco 7600 series routers, CSM, CSS, GSS, or VSS devices. Be sure to synchronize configurations on these devices after import, and whenever their configurations have been modified through the CLI.

The following require synchronization:

- Upgrading chassis hardware or software
- Adding new modules to the chassis
- Removing a module from a chassis
- Rearranging modules within the chassis
- Upgrading module software
- Changing the chassis configuration using the CLI instead of the ANM

Procedure

Step 1 Choose **Config > Devices > All Devices**.

The All Devices table appears.

Step 2 In the All Devices table, choose the device with the configuration that you want to synchronize, and click **CLI Sync**.

A popup confirmation window appears asking you to confirm the synchronization.

Step 3 In the confirmation window, click **OK** to synchronize the configuration or **Cancel** to cancel the synchronization.

ANM displays the status while synchronization is in progress and returns to the All Devices table when synchronization is complete.

Related Topics

- Configuring Devices, page 4-27
- Synchronizing Module Configurations, page 4-59
- Restarting Device Polling, page 4-66

Synchronizing Module Configurations

You can synchronize configurations for ACE modules or CSM modules when changes are made that have not been tracked in ANM.

The following module changes require synchronization:

- Upgrading module software
- Changing the module configuration using the CLI instead of the ANM

Procedure

Step 1 Choose **Config > Devices > All Devices**.

The All Devices table appears.

Step 2 In the All Devices table, choose the chassis that contains the module with the configuration that you want to synchronize, and click **Modules**.

The Modules table appears.

Step 3 In the Modules table, choose the module with the configuration you want to synchronize, and click **Sync**.

A popup confirmation window appears asking you to confirm the synchronization.

Step 4 In the confirmation window, click **OK** to synchronize the configuration or **Cancel** to cancel the synchronization.

ANM displays the status while synchronization is in progress and returns to the Modules table when synchronization is complete.

Related Topics

- Configuring Devices, page 4-27
- Managing Devices, page 4-58
- Synchronizing Device Configurations, page 4-58

Configuring User-Defined Groups

You can create logical groupings of virtual contexts or chassis for ease of management. These logical groups are known as *user-defined groups* and appear in the device tree (Config > Devices) in the folder named *Groups* for quick access.

Users can create their own groups, add and remove members, and assign group names that suit their environment and are meaningful to them.

This section includes the following topics:

- Adding a User-Defined Group, page 4-61
- Modifying a User-Defined Group, page 4-62
- Duplicating a User-Defined Group, page 4-62
- Deleting a User-Defined Group, page 4-63

Note Device groups continue to display device information even after you remove that device from ANM, which allows the device group information to be easily reassociated if you reimport the device. The device name must remain the same.

Adding a User-Defined Group

You can add a user-defined group.

Procedure

Step 1 Choose **Config > Devices > All Devices**.

The device tree appears.

Step 2 In the device tree, choose **Groups**.

The Groups table appears.

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

The Group configuration window appears.

Step 4 In the Name field of the Group configuration window, enter a unique name for this group.

Valid entries are unquoted text strings with no spaces and a maximum of 26 alphanumeric characters.

The window identifies the objects by type and provides a search field for each:

- Virtual Context Members
- Device Members
- Module Members
- CSM Members

Step 5 To add objects to the group, for each object type, choose the object in the Available Items list, and click **Add**.

The selected objects appear in the Selected Items list.

To remove objects that you do not want to include, choose the objects in the Selected Items list, and click **Remove**. The items then appear in the Available Items list.

To search for specific objects, enter a search string that contains the object name or part of the object name in the Search field, and then click **Search**. The Available Items list refreshes with the objects that meet the search criteria.

Step 6 In the Description field, enter a description for this group.

Step 7 Do one of the following:

- Click **Save** to accept your entries and to return to the Groups table.
- Click **Cancel** to exit this procedure without saving your entries and to return to the Groups table.

Related Topics

- Configuring User-Defined Groups, page 4-60
- Modifying a User-Defined Group, page 4-62
- Duplicating a User-Defined Group, page 4-62
- Deleting a User-Defined Group, page 4-63

Modifying a User-Defined Group

You can change the members or the description of a user-defined group. You cannot change the name of an existing user-defined group.

Procedure

Step 1 Choose **Config > Devices > All Devices**.

The device tree appears.

Step 2 In the device tree, click **Groups**.

The Groups table appears.

Step 3 In the Groups table, choose the group that you want to modify, and click **Edit**.

The Group configuration window appears.

Step 4 In each Members field of the Group configuration window, add or remove group members as follows:

- Choose the items that you want to add to this group in the Available Items list, and click **Add**.
- Choose the items that you want to remove from this group in the Selected Items list, and click **Remove**.

Step 5 In the Description field, modify the description as needed.

Step 6 Do one of the following:

- Click **Save** to accept your entries and to return to the Groups table.
- Click **Cancel** to exit this procedure without saving your entries and to return to the Groups table.

Related Topics

- Configuring User-Defined Groups, page 4-60
- Adding a User-Defined Group, page 4-61
- Duplicating a User-Defined Group, page 4-62
- Deleting a User-Defined Group, page 4-63

Duplicating a User-Defined Group

You can duplicate a user-defined group.

Procedure

Step 1 Choose **Config > Devices > All Devices**.

The device tree appears.

Step 2 In the device tree, click **Groups**.

The Groups table appears.

Step 3 In the Groups table, choose the user-defined group that you want to duplicate, and click **Duplicate**.

A popup window appears asking you to enter a new name.

Step 4 In the popup window, type the new group name, and click **OK**.

The Groups table refreshes and the duplicated group name appears in the list.

Related Topics

- Configuring User-Defined Groups, page 4-60
- Adding a User-Defined Group, page 4-61
- Modifying a User-Defined Group, page 4-62
- Deleting a User-Defined Group, page 4-63

Deleting a User-Defined Group

You can delete a user-defined group.

Procedure

Step 1 Choose **Config > Devices > All Devices**.

The device tree appears.

Step 2 In the device tree, click **Groups**.

The Groups table appears.

Step 3 In the Groups table, choose the user-defined group that you want to remove, and click **Delete**.

A popup confirmation window appears asking you to confirm the deletion.

Step 4 In the popup confirmation window, do one of the following:

- Click **OK** to delete the selected user-defined group.

  The Groups table refreshes and the deleted group no longer appears.
- Click **Cancel** to exit this procedure without deleting the group.

  The Groups table refreshes.

Related Topics

- Configuring User-Defined Groups, page 4-60
- Adding a User-Defined Group, page 4-61
- Modifying a User-Defined Group, page 4-62
- Duplicating a User-Defined Group, page 4-62

Updating Device Passwords

If you change the device password using the CLI, you can update the passwords in ANM without rediscovering or reimporting the chassis information. This includes the following devices that have been imported into ANM:

- ACE appliance
- Global Site Selector (GSS)
- Content Services Switch (CSS)
- Catalyst 6500 Virtual Switching System (VSS) 1440
- Catalyst 6500 series switch
- Cisco 7600 series router

Use this option to update the device password or enable password in ANM after they have been changed on the device.

Note the following usage guidelines when updating device passwords:

- When you update the password for an ACE appliance in the ANM server, ANM also sends the updated password to the device CLI and changes the password on the device.
- For the Catalyst 6500 chassis, Cisco 7600 series chassis, Catalyst 6500 Virtual Switching System (VSS), GSS, or CSS, the password changes made in the user interface apply to the ANM server only. Changing passwords in the Update Password window does not change the Password/Enable password on the device.

Procedure

Step 1 Choose **Config > Devices > All Devices**.

The All Devices table appears.

Step 2 In the All Devices table, choose the device with the passwords that you want to update in ANM, and click **Update Password**.

The Update Password window appears.

Step 3 In the Update Password window, update the device passwords in ANM using the information in Table 4-17.

Table 4-17 Update Chassis Password Options

Field	Description
Update	Passwords that you want to update in the ANM: • Both—Update both the device password and the device enable password. • Enable Password Only—Update the device enable password only. • Password Only—Update the device password only.
New Password	Updated device password.
Confirm New Password	Updated device password that you reenter.
New Enable Password	Updateddevice password.
Confirm New Enabled Password	Updated device password that you reenter.

Related Topics

- Changing ACE Module Passwords, page 4-65
- Managing Devices, page 4-58
- Configuring Devices, page 4-27

Changing ACE Module Passwords

You can change the ACE module card password. All ACE modules shipped from Cisco are configured with the same administrative username and password. Because this can compromise network security, we recommend that you change the username and passwords of the ACE modules after you import them into the ANM database.

Note This functionality is available only in Admin contexts.

Before You Begin

Import the ACE module into ANM and ensure that it is operational (see the "Adding ACE Modules to ANM" section on page 4-14).

Procedure

Step 1 Choose **Config > Devices > All Devices**.

The device tree appears.

Step 2 In the device tree, choose the chassis device containing the ACE module with the password that you want to change.

The Modules table appears.

Step 3 In the Modules table, choose the module whose password that you want to change, and click **Change Card Password**.

The Modules configuration window appears.

Step 4 In the Card Slot field, confirm that the correct module is selected.

Step 5 In the Card Type field, confirm that the correct version appears.

Step 6 In the Module Has Been Imported Into ANM field, confirm that the checkbox is checked to indicate that the module has been imported. This is a read-only field.

Step 7 In the Operation To Perform field, choose **Change card password**.

Step 8 In the User Name field, enter the username of the account whose password you want to change.

Step 9 In the Password field, enter the existing password for the account.

Step 10 In the New Password field, enter the new password for the account.

Valid passwords are unquoted text strings with a maximum of 64 characters. Reenter the password in the Confirm field.

Step 11 Do one of the following:

- Click **OK** to accept your entries and to return to the Modules table.
- Click **Cancel** to exit the procedure without saving your entries and to return to the Modules table.

Related Topics

- Configuring Devices, page 4-27
- Managing Devices, page 4-58
- Adding ACE Modules to ANM, page 4-14
- Updating Device Passwords, page 4-64

Restarting Device Polling

You can restart monitoring on a device that has stopped or failed to start.

Procedure

Step 1 Choose **Config > Devices > All Devices**.

The All Devices table appears.

Step 2 In the All Devices table, choose the device whose monitoring has stopped or failed, and click **Restart Polling**.

The All Devices table refreshes with updated polling status. For a description of the various polling status variables see Table 4-18 on page 4-67.

If ANM cannot monitor the selected device, it displays an error message stating the reason.

Related Topics

- Configuring Devices, page 4-27

- Adding and Managing Devices, page 4-1

Displaying All Devices

You can display all devices that have been imported into the ANM database.

Procedure

Step 1 Choose **Config > Devices**.

The device tree appears.

Step 2 In the device tree, choose **All Devices**.

The All Devices table displays information for the devices being managed by the ANM (see Table 4-18).

Table 4-18 All Devices Table Attributes

Field	Description
Name	Name assigned to the device.
Type	Type of the device, such as Chassis, ACE 4710, or CSS.
Version	Version of the software running on the device, if available.
IP Address	Device IP address.
Polling Status	Current polling status of the device: • Missing SNMP Credentials—SNMP credentials are not configured for this device; therefore, statistics are not collected. Add SNMPv2C credentials to fix this error. • Not Polled—SNMP polling has not started. Add SNMP V2C credentials to fix this error. • Monitoring Not Supported—This status appears at the device level only and applies to Catalyst 6500 series chassis, Cisco 7600 series routers, and ACE appliances. • Polling Failed—SNMP polling failed due to some internal error. Try enabling the SNMP collection again. • Polling Started—No action is required; everything is working properly. Polling states will display the activity. • Polling Timed Out—SNMP polling has timed out. This situation might occur if the wrong credentials were configured or an internal error exists, such as the SNMP protocol is configured incorrectly or the destination is not reachable. Verify that SNMP credentials are correct. If the problem persists, enable SNMP collection again. • Unknown—SNMP polling is not working due to one of the above-mentioned conditions. Check the SNMPv2C credential configuration.

Related Topics

- Adding and Managing Devices, page 4-1
- Configuring Catalyst 6500 Series Chassis and Cisco 7600 Series Router Primary Attributes, page 4-31

- Displaying Chassis Interfaces and Configuring High-Level Interface Attributes, page 4-34

Displaying Modules by Chassis

You can display all modules on a specific chassis.

Procedure

Step 1 Choose **Config > Devices > All Devices**.

The All Devices table appears.

Step 2 In the All Devices table, choose the chassis containing the modules that you want to view, and click **Modules**.

The Modules table appears, listing all modules on that chassis with the following information:

- Slot number
- Service module model
- Module type, such as Cisco Content Switching Module (CSM), ACE module and version, or other modules, such as supervisor modules
- Serial number
- Module operational state, such as Up, Powered Off, or Not Imported
- Version of software the module is running
- Brief description
- For ACE modules, the number of virtual contexts configured on the module
- For VSS devices, a Virtual Switch number column indicating the switch, slot, and port number. For example, command interface 1/5/4 specifies port 4 of the switching module in slot 5 of switch 1.

Depending on the type of module selected, such as CSM or ACE modules, the following options are available from this window:

- Import—Imports an ACE module that resides in the selected chassis but has not been imported into the ANM database. For more information, see the "Adding ACE Modules to ANM" section on page 4-14 or the "Importing CSM Devices" section on page 4-17.
- Change Card Password—Changes the administrative password on an ACE module that has been imported into the ANM database. For more information, see the "Changing ACE Module Passwords" section on page 4-65.
- Do Not Manage—Removes a selected ACE module from the ANM database. For more information, see the "Removing Modules from the ANM Database" section on page 4-69.

Step 3 (Optional) To display the modules of another chassis, choose another chassis in the device tree or use the chassis selector field at the top of the window.

Related Topics

- Displaying Chassis Interfaces and Configuring High-Level Interface Attributes, page 4-34
- Managing Catalyst 6500 Series Chassis or Cisco 7600 Series Router VLANs, page 4-40

- Adding ACE Modules to ANM, page 4-14
- Importing CSM Devices, page 4-17

Removing Modules from the ANM Database

You can remove a module from the ANM database.

Note If you physically replace an ACE module in a chassis, you need to synchronize the chassis in the ANM. See the "Synchronizing Chassis Configurations" section on page 4-59 for more information.

Procedure

Step 1 Choose **Config > Devices > All Devices**.

The All Devices table appears.

Step 2 In the All Devices table, choose the device containing the module that you want to remove, and click **Modules**.

The Modules table appears.

Step 3 In the Modules table, choose the module that you want to remove from ANM management, and click **Do Not Manage**.

The Modules configuration window appears.

Step 4 In the Modules configuration window, confirm the information in the following fields:

- Card Slot
- Card Type
- Module Has Been Imported Into ANM

Step 5 In the Operation To Perform field, choose **Do Not Manage**.

Step 6 Do one of the following:

- Click **OK** to confirm removal of the module.

  The Modules table refreshes and the removed module appears with the state Not Imported.

  You can import the module again when desired (see the "Adding ACE Modules to ANM" section on page 4-14).
- Click **Cancel** to exit the procedure without removing the ACE module and to return to the Modules table.

Related Topics

- Adding Network Devices into ANM, page 4-9
- Changing ACE Module Passwords, page 4-65