CHAPTER 5

Configuring Virtual Contexts

Date: 2/17/11

This chapter describes how to configure and manage the Cisco Application Control Engine (ACE) using Cisco Application Networking Manager (ANM).

This chapter includes the following sections:

Information About Virtual Contexts

Virtual contexts use the concept of virtualization to partition your ACE into multiple virtual devices or contexts. Each context contains its own set of policies, interfaces, resources, and administrators. This feature enables you to more closely and efficiently manage resources, users, and the services you provide to your customers.

There are two types of virtual contexts; the admin context and the user context. The ACE comes preconfigured with the default Admin context, which you can modify but you cannot delete. From the Admin context, you can create user contexts. You also use the Admin context to configure High Availability (HA or fault tolerance between ACE devices), configure resource classes, and manage ACE licenses.

Note If you restore the ANM database from a backup repository and if a virtual context that is in the repository has been removed from the device, ANM removes that context from the database and the context does not appear in the ANM interface.

Related Topics

- Creating Virtual Contexts, page 5-2
- Configuring Virtual Contexts, page 5-7
- Deleting Virtual Contexts, page 5-94
- Comparing Context and Building Block Configurations, page 5-88
- Restarting Virtual Context Polling, page 5-95
- Managing Virtual Contexts, page 5-90

Creating Virtual Contexts

You can create virtual contexts.

Note You must have the ability to create virtual contexts in your role and an Admin context in your domain before you can create virtual contexts. For more information about configuring roles and domains, see the “Managing User Roles” section on page 17-54 and the “Managing Domains” section on page 17-60.

Procedure

Step 1 Choose **Config > Devices**, and choose the ACE to which you want to add a virtual context.

The Virtual Contexts table appears.

Step 2 In the Virtual Contexts table, click **Add**.

The New Virtual Context window appears.

Step 3 Configure the virtual context using the information in Table 5-1.

Click **Basic Settings, Management Settings**, or **More Setting** to access the additional configuration attributes. By default, ANM hides the Management Settings and More Settings groups of configuration attributes until you specify a VLAN identifier in the Management Settings group.

Table 5-1 Virtual Context Configuration Attributes

Field	Description
Basic Settings	
Name	Unique name for the virtual context. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. This field is read-only for existing contexts.
Device	Device to associate with this context. This field appears for new contexts only.
Description	Brief description of the virtual context. Enter a description as an unquoted text string with a maximum of 240 alphanumeric characters.
Module	Field that appears when a chassis contains multiple ACE modules and for new contexts only. Choose the module to associate with this context.
Resource Class	Resource class that this virtual context is to use.
Allocated VLANs	Number of a VLAN or a range of VLANs used by the traffic that the context is to receive. You can specify VLANs in any of the following ways: • For a single VLAN, enter an integer from 2 to 4096. • For multiple, nonsequential VLANs, use comma-separated entries, such as 101, 201, 302. • For a range of VLANs, use the format <beginning-VLAN>-<ending-VLAN>, such as 101-150. **Note** VLANs cannot be modified in an Admin context.
Default Gateway IP	IP address of the default gateway. Use a comma-separated list to specify multiple IP addresses, such as 192.168.65.1, 192.168.64.2. Default static routes with a netmask and IP address of 0.0.0.0 previously configured on the ACE appear in this field.
Enable High Availability	Context to be used in a high availability (HA) group. **Note** This field is unavailable if the associated FT interface is not configured or if the ACE peer is not known. See Chapter 12, "Configuring High Availability" for details on ACE HA groups.
Management Settings	
VLAN Id	VLAN number that you want to assign to the management interface. Valid values are from 2 to 4094. The VLAN ID should be available in the allocated VLAN interface list. By default, all devices are assigned to VLAN1, known as the default VLAN. **Note** You must enter a VLAN ID before the other Management Settings attribute fields are enabled for configuring.
VLAN Description	Description for the management interface. Enter an unquoted text string that contains a maximum of 240 alphanumeric characters including spaces.

Table 5-1 Virtual Context Configuration Attributes (continued)

Field	Description
Interface Mode	Topology that reflects the relationship of the selected ACE virtual context to the real servers in the network: • **Routed**—The ACE virtual context acts as a router between the client-side network and the server-side network. In this topology, every real server for the application must be routed through the ACE virtual context, either by setting the default gateway on each real server to the virtual context server-side VLAN interface address, or by using a separate router with appropriate routes configured between the ACE virtual context and the real servers. • **Bridged**—The virtual ACE bridges two VLANs—a client-side VLAN and a real-server VLAN—on the same subnet using a bridged virtual interface (BVI). The real server routing does not change to accommodate the ACE virtual context. Instead the virtual ACE transparently handles traffic to and from the real servers.
Management IP	IP address that is to be used for remote management of the context. **Note** ANM considers an interface as a management interface if it has a management policy map associated with the VLAN interface. See the "Configuring VLAN Interfaces" section on page 11-5.
Management Netmask	Subnet mask to apply to this IP address.
Alias IP Address	IP address of the alias this interface is associated with.
Peer IP Address	IP address of the remote peer.
Access Permission	List of source IP addresses that are allowed on the management interface: • **Allow All**—Allows all configured client source IP addresses on the management interface as the network traffic matching criteria. • **Deny All**—Denies all configured client source IP addresses on the management interface as the network traffic matching criteria. • **Match**—Displays the Match Conditions table, where you specify the match criteria that the ACE is to use for traffic on the management interface.

Table 5-1 Virtual Context Configuration Attributes (continued)

Field	Description
Match Conditions	Match Conditions table that appears when you choose Match as the Access Permission selection. To add or modify the protocols allowed on this management VLAN, do the following: 1. Click **Add** to choose a protocol for the management interface, or choose an existing protocol entry listed in the Match Conditions table and click **Edit** to modify it. 2. In the Protocol drop-down list, choose a protocol: – **HTTP**—Specifies the Hypertext Transfer Protocol (HTTP). – **HTTPS**—Specifies the secure (SSL) Hypertext Transfer Protocol (HTTP) for connectivity with the ANM interface using port 443. – **ICMP**—Specifies the Internet Control Message Protocol (ICMP), commonly referred to as ping. – **KALAP-UDP**—Specifies the Keepalive Appliance Protocol over UDP. – **SNMP**—Specifies the Simple Network Management Protocol (SNMP). **Note** If SNMP is not selected, ANM will not be able to poll the context. – **SSH**—Specifies a Secure Shell (SSH) connection to the ACE. – **TELNET**—Specifies a Telnet connection to the ACE. – **XML-HTTPS**—Specifies HTTPS as the transfer protocol for sending and receiving XML documents between the ACE appliance and a Network Management System (NMS) using port 10443. This option is available for ACE appliances only. 3. In the Allowed From field, specify the matching criteria for the client source IP address: – **Any**—Specifies any client source address for the management traffic classification. – **Source Address**—Specifies a client source host IP address and subnet mask as the network traffic matching criteria. 4. Click **OK** to accept the protocol selection (or click **Cancel** to exit without accepting your entries). **Note** To remove a protocol from the management VLAN, choose the entry in the Match Conditions table, and click **Delete**.
Enable SNMP Get	Check box that you can check to add an SNMP Get community string to enable SNMP polling on this context.
SNMP v2c Read-Only Community String	Field that appears when you check the Enable SNMP Get check box. Enter the SNMPv2c read-only community string to be used as the SNMP Get community string.
Enable SNMP Trap	Check box that you can check to add an SNMP community string for ANM to receive traps from this context.
SNMP Community	Field that appears when you check the Enable SNMP Trap check box. Enter the SNMP version 1 or 2c read-only community string or the SNMP version 3 user name that is to be used as the SNMP trap.

Table 5-1 Virtual Context Configuration Attributes (continued)

Field	Description
Enable Syslog Notification	Check box that you can check to enable syslog logging or uncheck to disable syslog logging.
Add Admin User	Check box that you can check to add a user with an administrator role and default-domain access.
User Name	Field that appears when you check the Add Admin User check box. Specifies the name by which the user is to be identified (up to 24 characters). Only letters, numbers, and underscore can be used. The field is case sensitive.
Password	Field that appears when you check the Add Admin User check box. Enter the password for the Admin user account.
Confirm Password	Field that appears when you check the Add Admin User check box. Renter the password for the Admin user account.
More Settings	
Switch Mode	Feature that applies only to the ACE module software version A2(1.1) or later release. Choose Switch Mode to change the way that the ACE processes TCP connections that are not destined to a VIP or that do not have any policies associated with their traffic. For such traffic, the ACE still creates connection objects, but processes the connections as stateless connections, which means that they do not undergo any TCP normalization checks. With this option enabled, the ACE also creates stateless connections for non-SYN TCP packets if they satisfy all other configured requirements. This process ensures that a long-lived persistent connection passes through the ACE successfully (even if it times out) by being reestablished by any incoming packet related to the connection. By default, these stateless connections time out after 2 hours and 15 minutes unless you configure the inactivity timeout otherwise in a parameter map. When a stateless connection times out, the ACE does not send a TCP RST packet but silently closes the connection. Even though these connections are stateless, the TCP RST and FIN-ACK flags are honored and the connections are closed when the ACE sees these flags in the received packets.
Building Block To Apply	Configuration building block to apply to this context.

Step 4 Do one of the following:

- Click **Deploy Now** to deploy this context and save this configuration to the running-configuration and startup-configuration files. The window refreshes and you can continue with virtual context configuration (see the "Configuring Virtual Contexts" section on page 5-7).
- Click **Cancel** to exit this procedure without saving your entries. The Virtual Contexts table appears.

Related Topics

- Information About Virtual Contexts, page 5-2
- Configuring Virtual Contexts, page 5-7

Configuring Virtual Contexts

After creating a virtual context, you can configure it. Configuring a virtual context involves configuring a number of attributes, grouped into *configuration subsets*.

The options that appear when you choose Config > Devices **>** ***context*** depend on the following:

- Type of ACE device associated with the context: ACE module or ACE appliance.
- Role associated with your account, such as Admin, Network-Admin, or SSL-Admin.
- Context that you are configuring; an Admin context or a user context.

Table 5-2 describes configuration options for Admin contexts for ACE modules and ACE appliances although not all options are available for both types of devices.

Table 5-3 identifies the configuration options that are available for each ACE device type.

Note You cannot modify a virtual context when its CLI Sync Status is in the *Import Failed* state. You must synchronize the context before you can make changes to it. You can view CLI Sync Status and synchronize contexts from the Virtual Contexts table (Config > Devices > *ACE*).

Table 5-2 Virtual Context Configuration Options

Configuration Subset	Description	Related Topics
System	The System configuration subset includes the following: • Primary attributes such as building block, resource class, and VLAN options • Syslog attributes that allow you to identify the type and severity of syslog messages that are to be logged, the syslog log host, log messages, and log rate limits • SNMP attributes • Global policy maps for all VLANs on a virtual context • ACE license attributes that allow you to view, install, remove, update, and copy licenses for ACE hardware • Resource classes that allow you to manage virtual context access to individual ACE devices • Checkpoint (snapshot in time) of a known stable running configuration • Back up or restore the configuration and dependencies of an entire ACE or of a particular virtual context **Note** ACE licenses and resource classes can be configured in an Admin context only.	• Configuring Virtual Context Primary Attributes, page 5-12 • Configuring Virtual Context Syslog Settings, page 5-17 • Configuring SNMP for Virtual Contexts, page 5-25 • Applying a Policy Map Globally to All VLAN Interfaces, page 5-33 • Managing ACE Licenses, page 5-34 • Using Resource Classes, page 5-41 • Using the Configuration Checkpoint and Rollback Service, page 5-52 • Performing Device Backup and Restore Functions, page 5-56 • Performing Global Device Backup and Copy Functions, page 5-64

Table 5-2 Virtual Context Configuration Options (continued)

Configuration Subset	Description	Related Topics
Load Balancing	Load-balancing attributes allow you to do the following: • Configure virtual servers, real servers, and server farms for load balancing • Establish the predictor method and return code checking • Implement sticky groups for session persistence • Configure parameter maps to combine related actions for policy maps • Configure NAT so that only one address for the entire network to the outside world is advertised • Configure a secure keepalive-appliance protocol (KAL-AP) associated with a virtual context to enable communication between the ACE and a Global Site Selector (GSS)	• Information About Load Balancing, page 6-1 • Configuring Virtual Servers, page 6-2 • Configuring Server Farms, page 7-14 • Configuring Health Monitoring for Real Servers, page 7-30 • Configuring Sticky Groups, page 8-6 • Configuring Parameter Maps, page 9-1 • Configuring VLAN Interface NAT Pools, page 11-17 • Configuring Secure KAL-AP, page 7-54
SSL	Secure Sockets Layer (SSL) configuration options allow you to import and export SSL certificates and keys, set up SSL parameter maps and chain group parameters, generate certificate signing requests for submission to a certificate authority, authenticate peer certificates, and configure certificate revocation lists for use during client authentication. **Note** You cannot configure all SSL options in a building block. Instead, configure them in an Admin virtual context.	• Configuring SSL, page 10-1 • Using SSL Certificates, page 10-5 • Using SSL Keys, page 10-9 • Generating CSRs, page 10-24 • Configuring SSL Parameter Maps, page 10-17 • Configuring SSL Chain Group Parameters, page 10-21 • Configuring SSL Proxy Service, page 10-25 • Configuring SSL Authentication Groups, page 10-28 • Configuring CRLs for Client Authentication, page 10-29
Security	Security configuration options enable you to create access control lists, set access control list (ACL) attributes, resequence ACLs, delete ACLs, and configure object groups.	• Configuring Security with ACLs, page 5-68 • Creating ACLs, page 5-68 • Configuring Object Groups, page 5-79

Table 5-2 Virtual Context Configuration Options (continued)

Configuration Subset	Description	Related Topics
Network	Network configuration options allow you to configure the following: • VLAN interfaces • Bridged-group virtual interfaces (BVI) • Network Address Translation (NAT) pools for a VLAN interface • Static routes • Dynamic host configuration protocol (DHCP) relay agents • Port channel interfaces • Gigabit Ethernet interfaces • Over 8,000 static network address translation (NAT) configurations	• Configuring VLAN Interfaces, page 11-5 • Configuring Virtual Context BVI Interfaces, page 11-13 • Configuring VLAN Interface NAT Pools, page 11-17 • Configuring Virtual Context Static Routes, page 11-18 • Configuring Virtual Context BVI Interfaces, page 11-13 • Configuring Port-Channel Interfaces for the ACE Appliance, page 11-25 • Configuring Gigabit Ethernet Interfaces on the ACE Appliance, page 11-22 • Configuring Static VLANs for Over 8000 Static NAT Configurations, page 11-21
High Availability	High availability (HA) attributes allow you to configure two ACE devices for fault-tolerant redundancy and the tracking and detection of failures for timely switchover. **Note** You can set up high availability in an Admin context only.	• Configuring ACE High Availability, page 12-12 • Configuring ACE High Availability Peers, page 12-13 • Configuring High Availability Groups, page 12-15
HA Tracking and Failure Detection	HA tracking and failure detection attributes allow you to configure tracking processes that can help ensure reliable fault tolerance.	• High Availability Tracking and Failure Detection Overview, page 12-22 • Tracking VLAN Interfaces for High Availability, page 12-23 • Tracking Hosts for High Availability, page 12-24 • Configuring ACE HSRP Groups, page 12-28
Role-Based Access Control	Role-based access control (RBAC) attributes allow you to configure RBAC for individual virtual contexts. **Note** Virtual context RBAC is separate from ANM RBAC. For information about ANM RBAC, see the "How ANM Handles Role-Based Access Control" section on page 17-9.	• Configuring Device RBAC Users, page 4-45 • Configuring Device RBAC Roles, page 4-49 • Configuring Device RBAC Domains, page 4-53
Expert	Expert attributes allow you to configure traffic policies and configure optimization action lists.	• Configuring Virtual Context Class Maps, page 13-6 • Configuring Virtual Context Policy Maps, page 13-31 • Configuring an HTTP Optimization Action List, page 14-3

Table 5-3 Configuration Options by Device Type

Menu Option	ACE Device Type		Related Topic
	ACE 2.0	ACE 4710 Appliance	
System			
Primary Attributes	X	X	Configuring Virtual Context Primary Attributes, page 5-12
Syslog	X	X	Configuring Virtual Context Syslog Settings, page 5-17
SNMP	X	X	Configuring SNMP for Virtual Contexts, page 5-25
Global Policies	X	X	Applying a Policy Map Globally to All VLAN Interfaces, page 5-33
Licenses	X	X	Managing ACE Licenses, page 5-34
Application Acceleration and Optimization	–	X	Configuring Global Application Acceleration and Optimization, page 14-10
Resource Classes	X	X	Using Resource Classes, page 5-41
Checkpoints	X	X	Using the Configuration Checkpoint and Rollback Service, page 5-52
Backup/Restore	X	–	–
Load Balancing			
Virtual Servers	X	X	Configuring Virtual Servers, page 6-2
Real Servers	X	X	Configuring Real Servers, page 7-4
Server Farms	X	X	Configuring Server Farms, page 7-14
Health Monitoring	X	X	Configuring Health Monitoring for Real Servers, page 7-30
Stickiness	X	X	Configuring Sticky Groups, page 8-6
HTTP Parameter Maps	X	X	Configuring HTTP Parameter Maps, page 9-9
Connection Parameter Maps	X	X	Configuring Connection Parameter Maps, page 9-3
Optimization Parameter Maps	–	X	Configuring Optimization Parameter Maps, page 9-11
Generic Parameter Maps	X	X	Configuring Generic Parameter Maps, page 9-8
RTSP Parameter Maps	X	X	Configuring RTSP Parameter Maps, page 9-20
SIP Parameter Maps	X	X	Configuring SIP Parameter Maps, page 9-21
Skinny Parameter Maps	X	X	Configuring Skinny Parameter Maps, page 9-23
Secure KAL-AP	X	X	Configuring Secure KAL-AP, page 7-54
SSL			
Setup Sequence	X	X	SSL Setup Sequence, page 10-4
Certificates	X	X	Using SSL Certificates, page 10-5
Keys	X	X	Using SSL Keys, page 10-9
Parameter Map	X	X	Configuring SSL Parameter Maps, page 10-17
Chain Group Parameters	X	X	Configuring SSL Chain Group Parameters, page 10-21
CSR Parameters	X	X	Configuring SSL CSR Parameters, page 10-22
Proxy Service	X	X	Configuring SSL Proxy Service, page 10-25

Table 5-3 Configuration Options by Device Type (continued)

Menu Option	ACE Device Type		Related Topic
	ACE 2.0	ACE 4710 Appliance	
Auth Group Parameters	X	X	Configuring SSL Authentication Groups, page 10-28
Certificate Revocation Lists (CRLs)	X	X	Configuring CRLs for Client Authentication, page 10-29
Security			
ACLs	X	X	Creating ACLs, page 5-68
Object Groups	X	X	Configuring Object Groups, page 5-79
Network			
Port Channel Interfaces	–	X	Configuring Port-Channel Interfaces for the ACE Appliance, page 11-25
Gigabit Ethernet Interfaces	–	X	Configuring Gigabit Ethernet Interfaces on the ACE Appliance, page 11-22
VLAN Interfaces	X	X	Configuring VLAN Interfaces, page 11-5
BVI Interfaces	X	X	Configuring Virtual Context BVI Interfaces, page 11-13
NAT Pools	X	X	Configuring VLAN Interface NAT Pools, page 11-17
Static Routes	X	X	Configuring Virtual Context Static Routes, page 11-18
Global IP DHCP	X	X	Configuring Global IP DHCP, page 11-20
Static NAT Overwrite	X	–	Configuring Static VLANs for Over 8000 Static NAT Configurations, page 11-21
NAT Pools	X	X	Configuring VLAN Interface NAT Pools, page 11-17
High Availability			
Setup	X	X	Configuring ACE High Availability Peers, page 12-13
HA Tracking And Failure Detection			
Interfaces	X	X	Tracking VLAN Interfaces for High Availability, page 12-23
Hosts	X	X	Tracking Hosts for High Availability, page 12-24
HSRP Groups	X	X	Configuring ACE HSRP Groups, page 12-28
Role-Based Access Control			
Users	X	X	Configuring Device RBAC Users, page 4-45
Roles	X	X	Configuring Device RBAC Roles, page 4-49
Domains	X	X	Configuring Device RBAC Domains, page 4-53
Expert			
Class Maps	X	X	Configuring Virtual Context Class Maps, page 13-6
Policy Maps	X	X	Configuring Virtual Context Policy Maps, page 13-31
Action List	X	X	Configuring an HTTP Header Modify Action List, page 13-83 Configuring an HTTP Optimization Action List, page 14-3

Configuring Virtual Context System Attributes

This section shows how to configure the ACE virtual context system attributes, which are as follows:

- Virtual context primary attributes—See Configuring Virtual Context Primary Attributes, page 5-12.
- Syslog
  - Configuring Virtual Context Syslog Settings, page 5-17
  - Configuring Syslog Log Hosts, page 5-21
  - Configuring Syslog Log Messages, page 5-22
  - Configuring Syslog Log Rate Limits, page 5-24
- SNMP
  - Configuring SNMP for Virtual Contexts, page 5-25
  - Configuring SNMPv2c Communities, page 5-26
  - Configuring SNMPv3 Users, page 5-27
  - Configuring SNMP Trap Destination Hosts, page 5-29
  - Configuring SNMP Notification, page 5-31
- Global policy maps for all VLANs on a virtual context—See Applying a Policy Map Globally to All VLAN Interfaces, page 5-33.
- ACE licenses—See Managing ACE Licenses, page 5-34.
- ACE resource classes—See Using Resource Classes, page 5-41.

For ACE appliances, you can also configure global application acceleration and optimization. See the "Configuring Global Application Acceleration and Optimization" section on page 14-10.

Configuring Virtual Context Primary Attributes

Primary attributes allow you to configure essential information for each virtual context including a name, VLANs, a management IP address, and allowed protocols. After providing this information, you can configure other attributes, such as interfaces, load-balancing, or SSL. For a complete list of the configurable items, see the "Configuring Virtual Contexts" section on page 5-7.

Procedure

Step 1 Choose **Config** > **Devices** > *context* > **System** > **Primary Attributes**.

The Primary Attributes configuration window appears.

Step 2 In the Primary Attributes configuration window, enter the primary attributes for this virtual context using the information in Table 5-4.

Certain attribute fields are read-only for existing contexts.

Click **Basic Settings, Management Settings**, or **More Setting** to access the additional configuration attributes. By default, ANM hides these groups of configuration attributes.

Table 5-4 Primary Attributes Configuration Attributes

Field	Description
Basic Settings	
Name	Unique name for the virtual context. This field is read-only for existing contexts.
Description	Brief description of the virtual context. Enter a description as an unquoted text string with a maximum of 240 alphanumeric characters.
Resource Class	Resource class that this virtual context is to use. Click **View** to see the details of the selected resource class (Resource, Minimum, and Maximum).
Allocated VLANs	Number of a VLAN or a range of VLANs that contain traffic for the context to receive. You can specify VLANs in any of the following ways: • For a single VLAN, enter an integer from 2 to 4096. • For multiple, nonsequential VLANs, use comma-separated entries, such as 101, 201, 302. • For a range of VLANs, use the format <*beginning-VLAN*>-<*ending-VLAN*>*,* such as 101-150. **Note** VLANs cannot be modified in an Admin context. This field is read-only if configured for existing contexts.
Default Gateway IP	IP address of the default gateway. Use a comma-separated list to specify multiple IP addresses, such as 192.168.65.1, 192.168.64.2. Default static routes with a netmask and IP address of 0.0.0.0 previously configured on the ACE appear in this field.
Enable High Availability	Context for use in a high availability (HA) group. **Note** This field is unavailable if the associated FT interface is not configured or if the ACE peer is not known. See Chapter 12, "Configuring High Availability" for details on ACE HA groups.
Management Settings	
VLAN Id	VLAN number that you want to assign to the management interface. Valid values are from 2 to 4094. By default, all devices are assigned to VLAN1, known as the default VLAN. ANM identifies the management class maps and policy maps associated with the selected VLAN ID assigned to the management interface. This field is read-only if configured for existing contexts.
VLAN Description	Description for the management interface. Enter an unquoted text string that contains a maximum of 240 alphanumeric characters including spaces.

Table 5-4 Primary Attributes Configuration Attributes (continued)

Field	Description
Interface Mode	Topology that reflects the relationship of the selected ACE virtual context to the real servers in the network: • **Routed**—The ACE virtual context acts as a router between the client-side network and the server-side network. In this topology, every real server for the application must be routed through the ACE virtual context, either by setting the default gateway on each real server to the virtual context server-side VLAN interface address, or by using a separate router with appropriate routes configured between the ACE virtual context and the real servers. • **Bridged**—The virtual ACE bridges two VLANs—a client-side VLAN and a real-server VLAN—on the same subnet using a bridged virtual interface (BVI). In this case, the real server routing does not change to accommodate the ACE virtual context. Instead, the virtual ACE transparently handles traffic to and from the real servers. This field is read-only if configured for existing contexts.
Management IP	IP address that is to be used for remote management of the context. **Note** ANM considers an interface as a management interface if it has a management policy map associated with the VLAN interface. See the "Configuring VLAN Interfaces" section on page 11-5.
Management Netmask	Subnet mask to apply to this IP address.
Alias IP Address	IP address of the alias this interface is associated with.
Peer IP Address	IP address of the remote peer.
Access Permission	List of source IP addresses that are allowed on the management interface: • **Allow All**—Allows all configured client source IP addresses on the management interface as the network traffic matching criteria. • **Deny All**—Denies all configured client source IP addresses on the management interface as the network traffic matching criteria. • **Match**—Displays the Match Conditions table, where you specify the match criteria that the ACE is to use for traffic on the management interface.

Table 5-4 Primary Attributes Configuration Attributes (continued)

Field	Description
Match Conditions	Match Conditions table that appears when you choose Match as the Access Permission selection. To add or modify the protocols allowed on this management VLAN, do the following: 1. Click **Add** to choose a protocol for the management interface, or choose an existing protocol entry listed in the Match Conditions table and click **Edit** to modify it. 2. In the Protocol drop-down list, choose a protocol: – **HTTP**—Specifies the Hypertext Transfer Protocol (HTTP). – **HTTPS**—Specifies the secure (SSL) Hypertext Transfer Protocol (HTTP) for connectivity with the ANM interface using port 443. – **ICMP**—Specifies the Internet Control Message Protocol (ICMP), commonly referred to as ping. – **KALAP-UDP**—Specifies the Keepalive Appliance Protocol over UDP. – **SNMP**—Specifies the Simple Network Management Protocol (SNMP). **Note** If SNMP is not selected, ANM cannot poll the context. – **SSH**—Specifies a Secure Shell (SSH) connection to the ACE. – **TELNET**—Specifies a Telnet connection to the ACE. – **XML-HTTPS**—Specifies HTTPS as the transfer protocol for sending and receiving XML documents between the ACE appliance and a Network Management System (NMS) using port 10443. This option is available for ACE appliances only. 3. In the Allowed From field, specify the matching criteria for the client source IP address: – **Any**—Specifies any client source address for the management traffic classification. – **Source Address**—Specifies a client source host IP address and subnet mask as the network traffic matching criteria. 4. Click **OK** to accept the protocol selection (or click **Cancel** to exit without accepting your entries). **Note** To remove a protocol from the management VLAN, choose the entry in the Match Conditions table, and click **Delete**.
Enable SNMP Get	Check box to add an SNMP Get community string to enable SNMP polling on this context. This field is read-only if configured for existing contexts.
SNMP v2c Read-Only Community String	Field that appears when you check the Enable SNMP Get check box. Enter the SNMPv2c read-only community string to be used as the SNMP Get community string. This field is read-only if configured for existing contexts.
Enable SNMP Trap	Check box to add an SNMP community string for ANM to receive traps from this context. This field is read-only if configured for existing contexts.

Table 5-4 Primary Attributes Configuration Attributes (continued)

Field	Description
SNMP Community	Field that appears when you check the Enable SNMP Trap check box. Enter the SNMPv1 or SNMPv2c read-only community string or the SNMPv3 user name that is to be used as the SNMP trap. This field is read-only if configured for existing contexts.
Enable Syslog Notification	Check box to either enable or disable syslog logging.
More Settings	
Switch Mode	Feature that applies only to the ACE module software version A2(1.1) or later release. Choose Switch Mode to change the way that the ACE processes TCP connections that are not destined to a VIP or that do not have any policies associated with their traffic. For such traffic, the ACE still creates connection objects but processes the connections as stateless connections, which means that they do not undergo any TCP normalization checks. With this option enabled, the ACE also creates stateless connections for non-SYN TCP packets if they satisfy all other configured requirements. This process ensures that a long-lived persistent connection passes through the ACE successfully (even if it times out) by being reestablished by any incoming packet related to the connection. By default, these stateless connections time out after 2 hours and 15 minutes unless you configure the inactivity timeout otherwise in a parameter map. When a stateless connection times out, the ACE does not send a TCP RST packet but silently closes the connection. Even though these connections are stateless, the TCP RST and FIN-ACK flags are honored and the connections are closed when the ACE sees these flags in the received packets.
Shared VLAN Host Id	Specific bank of MAC addresses that the ACE uses. Enter a number from 1 to 16. Be sure to configure different bank numbers for multiple ACEs.
Tagged Building Block To Apply	Configuration building block to apply to this context.

Step 3 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 Virtual Contexts table.

Related Topics

- Information About Virtual Contexts, page 5-2
- Configuring VLAN Interfaces, page 11-5
- Configuring Virtual Context BVI Interfaces, page 11-13
- Configuring Virtual Context Syslog Settings, page 5-17
- Configuring Traffic Policies, page 13-1

Configuring Virtual Context Syslog Settings

The ANM uses syslog logging to send log messages to a process which logs messages to designated locations asynchronously to the processes that generated the messages.

Procedure

Step 1 Choose the item to configure:

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

The Syslog configuration window appears.

Step 2 In the Syslog configuration window, enter the syslog logging attributes in the displayed fields (see Table 5-6).

All fields that require you to choose syslog severity levels use the values in Table 5-5.

5-

Table 5-5 Syslog Logging Levels

Severity	Description
0-Emergency	Unusable system
1-Critical	Critical condition
2-Warning	Warning condition
3-Alert	Immediate action required
4-Error	Error condition
5-Notification	Normal but significant condition
6-Information	Informational message only
7-Debug	Appears only during debugging

The severity level that you specify indicates that you want syslog messages at that level and the more severe levels. For example, if you specify Error, syslog displays Error, Critical, Alert, and Emergency messages.

Note Setting all syslog levels to Debug during normal operations can degrade overall performance.

Table 5-6 Virtual Context Syslog Configuration Attributes

Field	Description	Action
Enable Syslog	Option that determines whether syslog logging is enabled or disabled.	Check the check box to enable syslog logging or clear the check box to disable syslog logging.
Facility	Syslog daemon that uses the specified syslog facility to determine how to process the messages it receives. Syslog servers file or direct messages based on the facility number in the message. For more information on the syslog daemon and facility levels, see your syslog daemon documentation.	Enter the facility appropriate for your network. Valid entries are 0 (LOCAL0) through 23 (LOCAL7). The default for ACE is 20 (LOCAL4).
Buffered Level	Option that enables system logging to a local buffer and limits the messages sent to the buffer based on severity.	Choose the desired level for sending system log messages to a local buffer. By default, logging to a buffer is disabled on the ACE.
Console Level	Option that specifies the maximum level for system log messages sent to the console.	Choose the desired level for sending system log messages to the console. By default, ACE does not display syslog messages during console sessions. **Note** Logging to the console can degrade system performance. We recommend that you log messages to the console only when you are testing or debugging problems. Do not use this option when the network is busy, because it can reduce ACE performance.
History Level	Option specifies the maximum level for system log messages sent as traps to an SNMP network management station.	Choose the desired level for sending system log messages as traps to an SNMP network management station. By default, the ACE does not send traps and inform requests to an SNMP network management station.
Monitor Level	Option that specifies the maximum level for system log messages sent to a remote connection using Secure Shell (SSH) or Telnet on the ACE.	Choose the desired level for sending system log messages to a remote connection using SSH or Telnet on the ACE. By default, logging to a remote connection using SSH or Telnet is disabled on the ACE. **Note** You must enable remote access on the ACE and establish a remote connection using the SSH or Telnet protocol from a PC for this option to work.

Table 5-6 Virtual Context Syslog Configuration Attributes (continued)

Field	Description	Action
Persistence Level	Option that specifies the maximum level for system log messages sent to Flash memory.	Choose the desired level for sending system log messages to Flash memory. By default, logging to Flash memory is disabled on the ACE. **Note** We recommend that you use a lower severity level, such as 3, because logging at a high rate to Flash memory on the ACE might impact performance.
Trap Level	Option that specifies the maximum level for system log messages sent to a syslog server.	Choose the desired level for sending system log messages to a syslog server. By default, logging to a syslog server is disabled on the ACE.
Supervisor Level	Option that specifies the maximum level for system log messages sent to the supervisor module on the Catalyst 6500 series chassis. **Note** This option does not appear for ACE appliances or ACE 4710-type configuration building blocks.	Choose the desired level for sending system log messages to the supervisor module on the Catalyst 6500 series chassis. **Note** We recommend that you use a lower severity level, such as 3, because logging at a high rate to the supervisor module might impact performance of the Catalyst 6500 series chassis.
Queue Size	Option that specifies the size of the queue for storing syslog messages in the message queue while they await processing.	Enter the desired queue size. Valid entries are from 0 to 8192 messages. The default is 80 messages.
Enable Timestamp	Option that determines whether syslog messages should include the date and time that the message was generated.	Choose the check box to enable time stamps on syslog messages or clear the check box to disable time stamps on syslog messages. By default, time stamps are not included on syslog messages.
Enable Standby	Option that determines whether or not logging is enabled or disabled on the failover standby ACE. When enabled: • This feature causes twice the message traffic on the syslog server. • The standby ACE syslog messages remain synchronized if failover occurs.	Choose the check box to enable logging on the failover standby ACE or clear the check box to disable logging on the failover standby ACE.
Enable Fastpath Logging	Option that determines whether or not connection setup and teardown messages are logged.	Check the check box to enable the logging of setup and teardown messages or clear the check box to disable the logging of setup and teardown messages. By default, the ACE does not log connection startup and teardown messages.

Table 5-6 Virtual Context Syslog Configuration Attributes (continued)

Field	Description	Action
Reject New Connection When TCP Queue Full	Option that indicates whether or not the ACE rejects new connections when the TCP queue is full.	This option is not applicable to ACE 4710 appliances running image A3(x.x). Check the check box to reject new connections when the syslog daemon can no longer reach the TCP syslog server. Clear the check box to disable this feature. This option is enabled by default.
Reject New Connection When Rate Limit Reached	Option that indicates whether or not the ACE rejects new connections when the syslog message rate is reached.	This option is not applicable to ACE 4710 appliances running image A3(x.x). Check the check box to reject new connections when the syslog message rate is reached. Clear the check box to disable this feature. This option is disabled by default.
Reject New Connection When Control Plane Buffer Full	Option that indicates whether or not the ACE rejects new connections when the syslog daemon buffer is full.	This option is not applicable to ACE 4710 appliances running image A3(x.x). Check the check box to reject new connections when the syslog daemon buffer is full. This option is disabled by default.
Device Id Type	Option that specifies the type of unique device identifier to be included in syslog messages sent to the syslog server. The device identifier does not appear in EMBLEM-formatted messages, SNMP traps, or on the ACE console, management session, or buffer.	Choose the type of device identifier to use: • **Any String**—Text string that you specify to uniquely identify the syslog messages sent from the ACE. If you choose this option, enter the text string to use in the Logging Device Id field. • **Context Name**—Name of the current virtual context used to uniquely identify the syslog messages sent from the ACE. • **Host Name**—Hostname of the ACE used to uniquely identify the syslog messages sent from the ACE. • **Interface**—IP address of the interface used to uniquely identify the syslog messages sent from the ACE. If you choose this option, enter the name of the interface in the Device Interface Name field. • **Undefined**—No identifier is used.

Table 5-6 Virtual Context Syslog Configuration Attributes (continued)

Field	Description	Action
Device Interface Name	Field that appears when the Device ID Type is Interface. This option specifies the interface to be used to uniquely identify syslog messages sent from the ACE.	Enter the device interface name to use to uniquely identify syslog messages sent from the ACE. Valid entries are 1 to 64 characters with no spaces. Syslog messages sent to an external server contain the IP address of the interface specified, regardless of which interface that the ACE uses to send the log data to the external server.
Logging Device Id	Field that appears when the Device ID Type is Any String. This option specifies the text string to use to uniquely identify syslog messages sent from the ACE.	Enter a text string that uniquely identifies the syslog messages sent from the ACE. The maximum string length is 64 characters without spaces. Do not use the following characters: & (ampersand), ‘ (single quote), “ (double quote), < (less than), > (greater than), or ? (question mark).

Step 3 Do the following:

- For virtual contexts, click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files, or choose another option to exit the procedure without saving your entries.
- For configuration building blocks, click **Save** to save your entries or **Cancel** to exit the procedure without saving your entries.

Related Topics

- Configuring Syslog Log Hosts, page 5-21
- Configuring Syslog Log Messages, page 5-22
- Configuring Syslog Log Rate Limits, page 5-24

Configuring Syslog Log Hosts

You can configure syslog log hosts. After configuring basic syslog characteristics (see the “Configuring Virtual Context Syslog Settings” section on page 5-17), you can configure the log host, log messages, and log rate limits.

Procedure

Step 1 Choose the item to configure:

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

The Syslog configuration window appears.

Step 2 In the Syslog configuration window, click the Log Host tab.

The Log Host table appears.

Step 3 In the Log Host table, click **Add** to add a new log host, or choose an existing log host, and click **Edit** to modify it.

The Log Host configuration window appears.

Step 4 In the Log Host configuration window IP Address field, enter the IP address of the host to use as the syslog server.

Step 5 In the Protocol field, choose TCP or UDP as the protocol to use.

Step 6 In the Protocol Port field, enter the number of the port that the syslog server listens to for syslog messages. Valid entries are from 1 to 65535.

Step 7 Check the Default UDP check box, which appears if TCP is selected in the Protocol field (Step 5), to specify that the ACE is to default to UDP if the TCP transport fails to communicate with the syslog server. Uncheck this check box to prevent the ACE from defaulting to UDP if the TCP transport fails.

Step 8 In the Format field, choose one of the following:

- **N/A** if you do not want to use EMBLEM-format logging.
- **Emblem** to enable EMBLEM-format logging for each syslog server.

  If you use Cisco Resource Manager Essentials (RME) software to collect and process syslog messages on your network, enable EMBLEM-format logging so that RME can handle them. Similarly, UDP needs to be enabled because the Cisco Resource Manager Essentials (RME) syslog analyzer supports only UDP syslog messages.

Step 9 Do one of the following:

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

Related Topics

- Configuring Virtual Context Syslog Settings, page 5-17
- Configuring Syslog Log Messages, page 5-22
- Configuring Syslog Log Rate Limits, page 5-24

Configuring Syslog Log Messages

You can configure syslog log messages. After configuring basic syslog characteristics (see the "Configuring Virtual Context Syslog Settings" section on page 5-17), you can configure the log host, log messages, and log rate limits.

Procedure

Step 1 Choose the item to configure:

- To configure a virtual context, choose **Config > Devices >** *context* **> System > Syslog**.

- To configure a configuration building block, choose **Config > Global > All Building Blocks >** *building_block* **> System > Syslog**.

The Syslog configuration window appears.

Step 2 In the Syslog configuration window, click the Log Message tab.

The Log Message table appears.

Step 3 In the Log Message table, click **Add** to add a new entry to this table, or choose an existing entry, and click **Edit** to modify it.

The Log Message configuration window appears.

Step 4 In the Message Id field, choose the system log message ID of the syslog messages that are to be sent to the syslog server or that are not to be sent to the syslog server.

Step 5 Check the Enable State check box to enable logging for the specified message ID or uncheck it to disable logging for the specified message ID.

If you check the Enable State check box, the Log Level field appears.

Step 6 In the Log Level field, choose the desired level of syslog messages to be sent to the syslog server, using the levels identified in Table 5-5.

Step 7 Do one of the following:

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

Related Topics

- Configuring Virtual Contexts, page 5-7
- Configuring Virtual Context Syslog Settings, page 5-17
- Configuring Syslog Log Hosts, page 5-21
- Configuring Syslog Log Rate Limits, page 5-24

Configuring Syslog Log Rate Limits

You can configure syslog log rate limits after configuring basic syslog characteristics (see the "Configuring Virtual Context Syslog Settings" section on page 5-17).

Procedure

Step 1 Choose the item to configure:

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

The Syslog configuration window appears.

Step 2 Click the Log Rate Limit tab.

The Log Rate Limit table appears.

Step 3 In the Log Rate Limit table, click **Add** to add a new entry to this table, or choose an existing entry, and click **Edit** to modify it.

The Log Rate Limit configuration window appears.

Step 4 In the Type field of the Log Rate Limit configuration window, choose the method by which syslog messages are to be limited:

- **Level**—Syslog messages are limited by syslog level. In the Level field, choose the level of syslog messages to be sent to the syslog server, using the levels identified in Table 5-5.
- **Message**—Syslog messages are limited by message identification number. In the Message Id field, choose the syslog message ID for those messages you want to suppress reporting.

Step 5 Check the Unlimited check box to apply no limits to system message logging or uncheck it to apply limits to system message logging.

If you uncheck the Unlimited check box, the Rate and Time Interval fields appear.

Step 6 (Optional) If you uncheck the Unlimited check box, specify the limits to apply to system message logging as follows:

a. In the Rate field, enter the number at which the system log messages are to be limited. When this limit is reached, the ACE rejects new syslog messages. Valid entries are from 0 to 2147483647.

b. In the Time Interval (Seconds) field, enter the length of time (in seconds) over which the system message logs are to be limited. For example, if you enter 42 in the Rate field and 60 in the Time Interval field, the ACE rejects any syslog messages that arrive after the first 42 messages in that 60-second period. Valid entries are from 0 to 2147483647 seconds.

Step 7 Do one of the following:

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

Related Topics

- Configuring Virtual Contexts, page 5-7
- Configuring Virtual Context Syslog Settings, page 5-17
- Configuring Syslog Log Hosts, page 5-21
- Configuring Syslog Log Messages, page 5-22

Configuring SNMP for Virtual Contexts

This section describes how to configure the SNMP attributes for a virtual context and contains the following topics:

- Configuring Basic SNMP Attributes, page 5-25
- Configuring SNMPv2c Communities, page 5-26
- Configuring SNMPv3 Users, page 5-27
- Configuring SNMP Trap Destination Hosts, page 5-29
- Configuring SNMP Notification, page 5-31

Configuring Basic SNMP Attributes

You can configure the basic SNMP attributes for use with a virtual context.

Procedure

Step 1 Choose the item to configure:

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

The SNMP configuration window appears.

Step 2 In the SNMP configuration window, configure the basic SNMP attributes using the information in Table 5-7.

Table 5-7 SNMP Attributes

Field	Description
Contact Information	Contact information for the SNMP server as a text string with a maximum of 240 characters including spaces. In addition to a name, you might want to include a phone number or e-mail address. If spaces are included, add quotation marks at the beginning and end of the entry.
Location	Physical location of the system as a text string with a maximum of 240 characters including spaces. If spaces are included, add quotation marks at the beginning and end of the entry.

Table 5-7 SNMP Attributes (continued)

Field	Description
Trap Source Interface	VLAN that identifies the interface from which SNMP traps originate.
IETF Trap	Check box to enable the ACE to send linkUp and linkDown traps with the IETF standard IF-MIB (RFC 2863) variable bindings, consisting of ifIndex, ifAdminStatus, and ifOperStatus. Uncheck the check box to not allow the ACE to send linkUp and linkDown traps with the IETF standard IF-MIB (RFC 2863) variable bindings. Instead, the ACE sends Cisco var-binds by default.

Step 3 Do one of the following:

- For virtual contexts, click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files, or choose another configuration option to exit the procedure without saving your entries.
- For configuration building blocks, click **OK** to save your entries or choose another configuration option to exit the procedure without saving your entries.

Related Topics

- Configuring Virtual Contexts, page 5-7
- Configuring SNMPv2c Communities, page 5-26
- Configuring SNMPv3 Users, page 5-27
- Configuring SNMP Trap Destination Hosts, page 5-29
- Configuring SNMP Notification, page 5-31

Configuring SNMPv2c Communities

You can configure SNMP communities for a virtual context or configuration building block after configuring basic SNMP information for a virtual context (see the "Configuring Basic SNMP Attributes" section on page 5-25).

Note All SNMP communities in ANM are read-only communities and all communities belong to the group *network monitors*.

Assumption

You have configured at least one SNMP contact (see Configuring Basic SNMP Attributes, page 5-25).

Procedure

Step 1 Choose the item to configure:

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

The SNMP configuration window appears.

Step 2 In the SNMP configuration window, click the SNMPv2c Configuration tab.

The SNMPv2c Configuration table appears.

Step 3 In the SNMPv2c Configuration table, click **Add** to add an SNMPv2c read-only community string.

The New SNMPv2c Configuration window appears.

Note You cannot modify an existing SNMPv2c community string. Instead, delete the existing SNMP v2c community string, and then add a new one.

Step 4 In the Read-Only Community field of the New SNMPv2c Configuration window, enter the SNMPv2c read-only community name.

Valid entries are unquoted text strings with no spaces and a maximum of 32 characters.

Step 5 Do one of the following:

- Click **Deploy Now** to immediately deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files. This option appears for virtual contexts.
- Click **OK** to save your entry. This option appears for configuration building blocks.
- Click **Cancel** to exit this procedure without saving your entry and to return to the SNMP v2c Community String table.
- Click **Next** to deploy your entry and to configure another SNMP community string. The window refreshes and you can enter another community string.

Related Topics

- Configuring Virtual Contexts, page 5-7
- Configuring Basic SNMP Attributes, page 5-25
- Configuring SNMPv3 Users, page 5-27
- Configuring SNMP Trap Destination Hosts, page 5-29
- Configuring SNMP Notification, page 5-31

Configuring SNMPv3 Users

You can configure SNMP version 3 users for a virtual context or configuration building block after configuring basic SNMP information for a virtual context (see the "Configuring Basic SNMP Attributes" section on page 5-25).

Assumption

You have configured at least one SNMP contact (see the "Configuring Basic SNMP Attributes" section on page 5-25).

Procedure

Step 1 Choose the item to configure:

- To configure a virtual context, choose **Config** > **Devices** > *context* > **System** > **SNMP**.

- To configure a configuration building block, choose **Config > Global > All Building Blocks >** *building_block* **> System > SNMP**.

The SNMP configuration window appears.

Step 2 In the SNMP configuration window, click the SNMPv3 Configuration tab.

The SNMP v3 Configuration table appears.

Step 3 In the SNMP v3 Configuration table, click **Add** to add users, or choose an existing entry in the SNMPv3 Configuration table, and click **Edit** to modify it.

The SNMP v3 Configuration window appears.

Step 4 In the SNMP v3 Configuration window, enter SNMP user attributes using the information in Table 5-8.

Table 5-8 SNMP User Configuration Attributes

Field	Description
User Name	SNMP username. Valid entries are unquoted text strings with no spaces and a maximum of 24 characters.
Authentication Algorithm	Authentication algorithm to be used for this user: • **N/A**—No authentication algorithm is used. • **Message Digest 5 (MD5)**—Message Digest 5 is used as the authentication mechanism. • **Secure Hash Algorithm (SHA)**—Secure Hash Algorithm is used as the authentication mechanism.
Authentication Password	Field that appears if you choose an authentication algorithm. Enter the authentication password for this user. Valid entries are unquoted text strings with no spaces. This password can have a minimum of 8 characters. If use of a localized key is disabled or N/A, you can enter a maximum of 64 characters. If use of a localized key is enabled, you can enter a maximum of 130 characters. The ACE automatically updates the password for the CLI user with the SNMP authentication password.
Confirm	Field that appears if you choose an authentication algorithm. Reenter the authentication password.
Localized	Field that appears if you choose an authentication algorithm. Specify whether or not the password is in localized key format for security encryption: • **N/A**—This option is not configured. • **False**—The password is not in localized key format for encryption. • **True**—The password is in localized key format for encryption.
Privacy	Field that appears if you choose an authentication algorithm. Specify whether or not encryption attributes are to be configured for this user: • **N/A**—This option is not configured. • **False**—Encryption parameters are not to be configured for this user. • **True**—Encryption parameters are to be configured for this user.

Table 5-8 SNMP User Configuration Attributes (continued)

Field	Description
AES 128	Field that appears if you set Privacy to True. Indicate whether the 128-byte Advanced Encryption standard (AES) algorithm is to be used for privacy. AES is a symmetric cipher algorithm and is one of the privacy protocols for SNMP message encryption. Choices are as follows: • **N/A**—This option is not configured. • **False**—AES 128 is not used for privacy. • **True**—AES 128 is used for privacy.
Privacy Password	Field that appears if you set Privacy to True. Enter the user encryption password. This password can have a minimum of 8 characters. If the passphrases are specified in clear text, you can enter a maximum of 64 characters. If use of a localized key is enabled, you can enter a maximum of 130 characters. Spaces are not allowed.
Confirm	Field that appears if you set Privacy to True. Reenter the privacy password.

Step 5 Do one of the following:

- Click **Deploy Now** to immediately deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files. This option appears for virtual contexts.
- Click **OK** to save your entries. This option appears for configuration building blocks.
- Click **Cancel** to exit this procedure without saving your entries and to return to the SNMP v3 Configuration table.
- Click **Next** to deploy your entries and to add another entry to the SNMP v3 Configuration table. The window refreshes and you can enter another SNMP v3 user.

Related Topics

- Configuring Virtual Contexts, page 5-7
- Configuring Basic SNMP Attributes, page 5-25
- Configuring SNMPv2c Communities, page 5-26
- Configuring SNMP Trap Destination Hosts, page 5-29
- Configuring SNMP Notification, page 5-31

Configuring SNMP Trap Destination Hosts

You can configure SNMP trap destination hosts for a virtual context after configuring basic SNMP information for a virtual context (see the “Configuring Basic SNMP Attributes” section on page 5-25).

To receive SNMP notifications you must configure the following attributes:

- At least one SNMP trap destination host.
- At least one type of notification (see the “Configuring SNMP Notification” section on page 5-31).

Assumption

You have configured at least one SNMP contact (see the "Configuring Basic SNMP Attributes" section on page 5-25).

Procedure

Step 1 Choose the item to configure:

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

The SNMP configuration window appears.

Step 2 In the SNMP configuration window, click the Trap Destination Host tab.

The Trap Destination Host table appears.

Step 3 In the Trap Destination Host table, click **Add** to add a host, or choose an existing entry in the table, and **Edit** to modify it.

The Trap Destination Host configuration window appears.

Step 4 In the IP Address field of the Trap Destination Host configuration window, enter the IP address of the server that is to receive SNMP notifications.

Enter the address in dotted-decimal format, such as 192.168.11.1.

Step 5 In the Port field, enter the port to use.

The default port is 162.

Step 6 In the Version field, choose the version of SNMP used to send traps:

- **V1**—SNMPv1 is used to send traps. This option is not available for use with SNMP inform requests.
- **V2c**—SNMPv2c is used to send traps.
- **V3**—SNMPv3 is used to send traps. This version is the most secure model because it allows packet encryption.

Step 7 In the Community field, enter the SNMP community string or username to be sent with the notification operation.

Valid entries are unquoted text strings with no spaces and a maximum of 32 characters.

Step 8 Do one of the following:

- Click **Deploy Now** to immediately deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files. This option appears for virtual contexts.
- Click **OK** to save your entries. This option appears for configuration building blocks.
- Click **Cancel** to exit this procedure without saving your entries and to return to the Trap Destination Host table.
- Click **Next** to deploy your entries and to add another entry to the Trap Destination Host table. The window refreshes and you can add another trap destination host.

Related Topics

- Configuring Virtual Contexts, page 5-7
- Configuring Basic SNMP Attributes, page 5-25

- Configuring SNMPv2c Communities, page 5-26
- Configuring SNMPv3 Users, page 5-27
- Configuring SNMP Notification, page 5-31

Configuring SNMP Notification

You can configure SNMP notification for a virtual context after configuring basic SNMP information for a virtual context (see the "Configuring Basic SNMP Attributes" section on page 5-25).

To receive SNMP notifications you must configure the following attributes:

- At least one SNMP trap destination host (see the "Configuring SNMP Trap Destination Hosts" section on page 5-29).
- At least one type of notification.

Assumptions

- You have configured at least one SNMP contact (see the "Configuring Basic SNMP Attributes" section on page 5-25).
- At least one SNMP server host has been configured (see the "Configuring SNMP Trap Destination Hosts" section on page 5-29).

Procedure

Step 1 Choose the item to configure:

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

The SNMP configuration window appears.

Step 2 In the SNMP configuration window, click the SNMP Notification tab.

The SNMP Notification table appears.

Step 3 In the SNMP Notification table, click **Add** to add a new entry, or choose an existing entry in the table, and click **Edit** to modify it.

The SNMP Notification configuration window appears.

Step 4 In the Options field of the SNMP Notification configuration window, choose the type of notifications to be sent to the SNMP host.

Some options are available only in the Admin context.

Note When configuring SNMP notification for ACE appliances, we recommend that you choose the more specific options. For example, choose Slb real or Slb vserver instead of Slb to ensure that the correct commands are issued on the ACE appliance.

Choices are as follows:

- **License**—SNMP license notifications are to be sent. This option is available only in the Admin context.
- **SLB**—Server load-balancing notifications are to be sent.

- **SLB Real Server**—Notifications of real server state changes are to sent.
- **SLB Virtual Server**—Notifications of virtual server state changes are to be sent.
- **SNMP**—SNMP notifications are to be sent.
- **SNMP Authentication**—Notifications of incorrect community strings in SNMP requests are to be sent.
- **SNMP Cold-Start**—SNMP agent restart notifications are to be sent after a cold restart (full power cycle) of the ACE. This option is available only in the Admin context.
- **SNMP Link-Down**—Notifications are to be sent when a VLAN interface is down.
- **SNMP Link-Up**—Notifications are to be sent when a VLAN interface is up.
- **Syslog**—Error message notifications (Cisco Syslog MIB) are to be sent.
- **Virtual Context**—Virtual context notifications are to be sent.

Step 5 Do one of the following:

- Click **Deploy Now** to immediately deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files. This option appears for virtual contexts.
- Click **OK** to save your entries. This option appears for configuration building blocks.
- Click **Cancel** to exit this procedure without saving your selection and to return to the SNMP Notification table.
- Click **Next** to deploy your entries and to add another entry to the SNMP Notification table. The window refreshes and you can choose another SNMP notification option.

Related Topics

- Configuring Virtual Contexts, page 5-7
- Configuring Basic SNMP Attributes, page 5-25
- Configuring SNMPv2c Communities, page 5-26
- Configuring SNMPv3 Users, page 5-27
- Configuring SNMP Trap Destination Hosts, page 5-29

Applying a Policy Map Globally to All VLAN Interfaces

You can apply a policy map globally to all VLAN interfaces in a selected context or configuration building block.

To apply a policy map to a specific context VLAN interface only, see the Input Policies attribute in the "Configuring VLAN Interfaces" section on page 11-5.

Note You cannot modify a policy map that is currently applied to an interface. To modify an applied policy map, you must first remove (delete) it from the interface, make the required modifications, and then apply it to the interface again.

Assumption

A Layer 3/Layer 4 or Management policy map has been configured for the selected context or building block. For more information, see the "Configuring Virtual Context Policy Maps" section on page 13-31.

Procedure

Step 1 Choose the item to configure:

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

The Global Policies table appears.

Step 2 In the Global Policies table, click **Add** to add a new global policy.

The New Global Policy window appears.

Step 3 In the Policy Map field of the New Global Policy window, choose an existing policy map that you want to apply to all VLANs in this context.

Note The Direction field displays the value "input" and cannot be modified.

Step 4 Do one of the following:

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

Related Topics

- Information About Virtual Contexts, page 5-2
- Configuring Virtual Context Primary Attributes, page 5-12
- Configuring VLAN Interfaces, page 11-5

- Configuring Virtual Context Syslog Settings, page 5-17
- Configuring Traffic Policies, page 13-1

Managing ACE Licenses

Note This functionality is available for only Admin contexts.

Cisco offers licenses for ACE modules and appliances that allow you to increase the number of default contexts, bandwidth, and SSL transactions per second (TPS). For more information about these licenses, see the Cisco Application Control Engine documentation on Cisco.com.

If you install ACE licenses to increase the number of virtual contexts that you can create and manage on a device, you need to ensure that the installed ANM licenses support the increased number of virtual contexts. For example, if you install an upgrade ACE device license that allows you to create and manage 20 virtual contexts on the device, you must purchase and install the appropriate ANM license before you can manage the additional contexts using ANM. For more information about using and managing ANM licenses, see the "Managing ANM Licenses" section on page 17-74.

You can view, install, remove, or update ACE device licenses using ANM.

This section includes the following topics:

- Viewing ACE Licenses, page 5-34
- Installing ACE Licenses, page 5-35
- Uninstalling ACE Licenses, page 5-37
- Updating ACE Licenses, page 5-38
- Displaying the File Contents of a License, page 5-40

Viewing ACE Licenses

Note This functionality is available for only Admin contexts.

You can view the licenses that are currently installed on an ACE.

Procedure

Step 1 Choose **Config > Devices**.

The device tree appears.

Step 2 In the device tree, choose the Admin context with the ACE licenses that you want to view, and click **System > Licenses**.

The following license tables appear:

- License Status Table—Provides a summary of the license status for the ACE, including:
  - SSL transactions per second
  - Number of supported virtual contexts

  - ACE bandwidth in gigabits per second

  For ACE appliances, it also displays the following:

  - Compression performance in megabits or gigabits per second
  - Web optimization in the number of connections per second

- Installed License Files Table—Lists all installed licenses with their filenames, vendors, and expiration dates.

Related Topics

- Managing ACE Licenses, page 5-34
- Installing ACE Licenses, page 5-35
- Uninstalling ACE Licenses, page 5-37
- Updating ACE Licenses, page 5-38
- Displaying the File Contents of a License, page 5-40

Installing ACE Licenses

Note This functionality is available for only Admin contexts.

You can install an ACE license on the device after you copy the license from a remote network server to the disk0: file system in Flash memory on the ACE. You can use the ANM to perform both processes from a single dialog box. If you previously copied the license to disk0: on the ACE by using the **copy disk0:** CLI command, you can use this dialog box to install the new license or upgrade license on your ACE.

Assumption

This topic assumes the following:

- You have received the proper software license key for the ACE.
- ACE licenses are available on a remote server for importing to the ACE, or you have received the software license key and have copied the license file to the disk0: filesystem on the ACE using the **copy disk0:** CLI command. See either the *Cisco Application Control Engine Module Administration Guide* or *Cisco 4700 Series Application Control Engine Appliance Administration Guide* for details.

Procedure

Step 1 Choose **Config > Devices**.

The device tree appears.

Step 2 In the device tree, choose the Admin context that you want to import and install a license for, and click **System > Licenses**.

The following license tables appear:

- License Status Table—Provides a summary of the license status for the ACE, including:
  - SSL transactions per second
  - Number of supported virtual contexts
  - ACE bandwidth in gigabits per second

  For ACE appliances, it also displays the following:
  - Compression performance in megabits or gigabits per second
  - Web optimization in the number of connections per second
- Installed License Files Table—Lists all installed licenses with their filenames, vendors, and expiration dates.

Step 3 Click **Install**.

The Install an ACE License dialog box appears.

Step 4 (Optional) If the license currently exists on the ACE disk0: file system in Flash memory, do the following:

a. In the Select an Option to Locate a License File section of the dialog box, click the **Select a license file on the ACE** option.

b. In the Select a License File on the Device (disk0) section of the dialog box, from the drop-down list, choose the name of the license file.

c. Go to Step 10.

Step 5 (Optional) If the license must be copied to the disk0: file system in Flash memory, in the Select an Option to Locate a License File section of the dialog box, click the **Import a license file from remote system** option. Go to Step 6.

Step 6 In the Protocol To Connect To Remote System field, choose the protocol to be used to import the license file from the remote server to the ACE as follows:

- If you choose FTP, the User Name and Password fields appear. Go to Step 7.
- If you choose SFTP, the User Name and Password fields appear. Go to Step 7.
- If you choose TFTP, go to Step 8.

Step 7 (Optional) If you choose FTP or SFTP, do the following:

a. In the User Name field, enter the username of the account on the network server.

b. In the Password field, enter the password for the user account.

Step 8 In the Remote System IP Address field, enter the host IP address of the remote server.

For example, your entry might be 192.168.11.2.

Step 9 In the License Path In Remote System field, enter the host path and filename of the license file on the remote server in the format */path/filename* where:

- *path* represents the directory path of the license file on the remote server.
- *filename* represents the filename of the license file on the remote server.

For example, your entry might resemble /usr/bin/ACE-VIRT-020.lic.

Step 10 Do one of the following:

- Click **Install** to accept your entries and to install the license file.
- Click **Cancel** to exit this procedure without installing the license file and to return to the Licenses table.

Step 11 (Optional) After installing an ACE license, Cisco recommends that you manually synchronize the ACE Admin context with the CLI to ensure that ANM accurately displays the monitored resource usage information (Monitor > Devices > ACE > Resource Usage > Connections).

For information about synchronizing the Admin context, see the "Synchronizing Virtual Context Configurations" section on page 5-92.

Related Topics

- Managing ACE Licenses, page 5-34
- Viewing ACE Licenses, page 5-34
- Uninstalling ACE Licenses, page 5-37
- Updating ACE Licenses, page 5-38
- Displaying the File Contents of a License, page 5-40

Uninstalling ACE Licenses

Note This functionality is available for Admin contexts only.

You can remove ACE licenses.

Caution Removing licenses can affect the ACE bandwidth or performance. For detailed information on the effect of license removal on the ACE, see the Cisco Application Control Engine documentation on Cisco.com.

Procedure

Step 1 Choose **Config > Devices**.

The device tree appears.

Step 2 In the device tree, choose the Admin context with the license that you want to remove, and click **System > Licenses**.

Step 3 In the Installed License Files table, choose the license to be removed.

Step 4 Click **Uninstall**.

A dialog box appears, asking you to confirm the license removal process.

Note Before continuing, confirm that you have selected the correct license to be removed. When you click **OK** in the confirmation window, you cannot stop the removal process.

Note Removing licenses can affect the number of contexts, ACE bandwidth, or SSL TPS (transactions per second). Be sure you understand the effect on your environment before removing the license.

Step 5 Click **OK** to confirm the removal or **Cancel** to stop the removal process.

If you click **OK**, a status window appears with the status of license removal. When the license has been removed, the License table refreshes without the deleted license.

Step 6 (Optional) After uninstalling an ACE license, Cisco recommends that you manually synchronize the ACE Admin context with the CLI to ensure that ANM accurately displays the monitored resource usage information (Monitor > Devices > ACE > Resource Usage > Connections).

For information about synchronizing the Admin context, see the "Synchronizing Virtual Context Configurations" section on page 5-92.

Related Topics

- Managing ACE Licenses, page 5-34
- Installing ACE Licenses, page 5-35
- Viewing ACE Licenses, page 5-34
- Updating ACE Licenses, page 5-38
- Displaying the File Contents of a License, page 5-40

Updating ACE Licenses

Note This functionality is available for Admin contexts only.

You can convert demonstration licenses to permanent licenses and to upgrade permanent licenses to increase the number of virtual contexts.

Assumption

This topic assumes the following:

- You have received the updated software license key for the ACE.
- ACE licenses are available on a remote server for importing to the ACE, or you have received the updated software license key and have copied the license file to the disk0: filesystem on the ACE using the **copy disk0:** CLI command. See either the *Cisco Application Control Engine Module Administration Guide* or *Cisco 4700 Series Application Control Engine Appliance Administration Guide* for details.

Procedure

Step 1 Choose **Config > Devices**.

The device tree appears.

Step 2 In the device tree, choose the Admin context with the license that you want to update, and click **System > Licenses**.

The following license tables appear:

- License Status Table—Provides a summary of the license status for the ACE, including:
  - SSL transactions per second
  - Number of supported virtual contexts
  - ACE bandwidth in gigabits per second

  For ACE appliances, it also displays the following:
  - Compression performance in megabits or gigabits per second
  - Web optimization in the number of connections per second
- Installed License Files Table—Lists all installed licenses with their filenames, vendors, and expiration dates.

Step 3 Choose the license to be updated, and click **Update**.

The Update License dialog box appears.

Step 4 (Optional) If the update license currently exists on the ACE disk0: file system in Flash memory, do the following:

a. In the Select an Option to Locate a License File section of the dialog box, click the **Select a license file on the ACE** option.

b. In the Select a License File on the Device (disk0) section of the dialog box, choose the name of the update license file from the drop-down list.

c. Go to Step 10.

Step 5 (Optional) If the update license must be copied to the disk0: file system in Flash memory, in the Select an Option to Locate a License File section of the dialog box, click the **Import a license file from remote system** option. Go to Step 6.

Step 6 In the Protocol To Connect To Remote System field, choose the protocol to be used to import the update license file from the remote server to the ACE as follows:

- If you choose FTP, the User Name and Password fields appear. Go to Step 7.
- If you choose SFTP, the User Name and Password fields appear. Go to Step 7.
- If you choose TFTP, go to Step 8.

Step 7 (Optional) If you choose FTP or SFTP, do the following:

a. In the User Name field, enter the username of the account on the network server.

b. In the Password field, enter the password for the user account.

Step 8 In the Remote System IP Address field, enter the host IP address of the remote server.

For example, your entry might be 192.168.11.2.

Step 9 In the Licence Path In Remote System field, enter the host path and filename of the license file on the remote server in the format */path/filename* where:

- *path* represents the directory path of the license file on the remote server.
- *filename* represents the filename of the license file on the remote server.

For example, your entry might be /usr/bin/ACE-VIRT-020.lic.

Step 10 Do one of the following:

- Click **Update** to update the license and to return to the License table. The License table displays the updated information.
- Click **Cancel** to exit this procedure without updating the license and to return to the License table.

Step 11 (Optional) After updating an ACE license, Cisco recommends that you manually synchronize the ACE Admin context with the CLI to ensure that ANM accurately displays the monitored resource usage information (Monitor > Devices > ACE > Resource Usage > Connections).

For information about synchronizing the Admin context, see the "Synchronizing Virtual Context Configurations" section on page 5-92.

Related Topics

- Managing ACE Licenses, page 5-34
- Installing ACE Licenses, page 5-35
- Viewing ACE Licenses, page 5-34
- Uninstalling ACE Licenses, page 5-37
- Displaying the File Contents of a License, page 5-40

Displaying the File Contents of a License

Note This functionality is available for only Admin contexts.

You can display file content information about ACE licenses.

Procedure

Step 1 Choose **Config > Devices**.

The device tree appears.

Step 2 Choose the Admin context with the license information that you want to view, and choose **System > Licenses**.

The following two license tables appear:

- License Status Table—Provides a summary of the license status for the ACE, including the supported features and capabilities.
- Installed License Files Table—Lists all installed licenses with their filenames, vendors, and expiration dates.

Step 3 Choose the installed license file with the information that you want to display, and click **View**.

ANM displays the output of the **show license file** C LI command.

For example:

```
SERVER this_host ANY
     VENDOR cisco
     INCREMENT ACE-AP-C-2000-LIC cisco 1.0 permanent 1 \
             NOTICE="<LicFileID>lic.conf</LicFileID><LicLineID>0</LicLineID> \
<PAK>dummyPak</PAK>" SIGN=BBBDC344EAE8
```

Step 4 Click **Close** when you finish viewing the license file information.

Related Topics

- Managing ACE Licenses, page 5-34
- Installing ACE Licenses, page 5-35
- Viewing ACE Licenses, page 5-34
- Uninstalling ACE Licenses, page 5-37

Using Resource Classes

Resource classes are the means by which you manage virtual context access to ACE resources, such as concurrent connections or bandwidth rate. ACE devices are preconfigured with a default resource class that is applied to the Admin context and any user context upon creation. The default resource class is configured to allow a context to operate within a range that can vary from no resource access (0%) to complete resource access (100%). When you use the default resource class with multiple contexts, you run the risk of oversubscribing ACE resources. This means that the ACE permits all contexts to have full access to all resources on a first-come, first-served basis. When a resource is utilized to its maximum limit, the ACE denies additional requests made by any context for that resource.

To avoid oversubscribing resources and to help guarantee access to a resource by any context, you can create customized resource classes that you associate with one or more contexts. A context becomes a member of the resource class when you make the association. Creating a resource class allows you to set limits on the minimum and maximum amounts of each ACE resource that a member context is entitled to use. You define the minimum and maximum values as a percentage of the whole. For example, you can create a resource class that allows its member contexts access to no less that 25% of the total number of SSL connections that the ACE supports.

You can limit and manage the allocation of the following ACE resources:

- ACL memory
- Buffers for syslog messages and TCP out-of-order (OOO) segments
- Concurrent connections (through-the-ACE traffic)
- Management connections (to-the-ACE traffic)
- Proxy connections
- Set resource limit as a rate (number per second)
- Regular expression (regexp) memory
- SSL connections
- Sticky entries
- Static or dynamic network address translations (Xlates)

When you discover ACE devices, the ANM detects the resource class information and imports it with other device information. If an ACE is not configured for a resource class, it inherits the resource class configuration of the virtual context it is associated with. If an ACE does have a resource class configuration but it differs from one configured in the ANM, the discrepancy is logged as an anomaly but otherwise has no impact on the import process or the ACE.

Table 5-9 identifies and defines the resources that you can establish for resource classes.

Related Topics

- Global and Local Resource Classes, page 5-42
- Resource Allocation Constraints, page 5-42
- Using Global Resource Classes, page 5-44
- Displaying Local Resource Class Use on Virtual Contexts, page 5-52

Global and Local Resource Classes

ANM provides two levels of resource classes for ACE devices that operate independently of each other:

- Local or device-specific resource classes
- Global resource classes

Local resource classes are initially imported from the ACE during the import process and appear in the ANM interface in the Admin virtual context where they can be managed, modified, or deleted by an Admin user. An Admin user can also create new, local resources classes by using ANM. Choose **Config > Devices >** *Admin_context* **> System > Resource Classes** to add, view, or modify local resource classes.

Global resource classes are managed separately from local resource classes and require manual deployment to a specific ACE using the Admin virtual context before they take effect. If you deploy a global resource class to an ACE that does not have a resource class with the same name, ANM creates a new local resource class with the same name and properties as the global resource class. If you deploy a global resource class to an ACE that already has a resource class with the same name, ANM replaces the properties of the local resource class with the properties from the global resource class. Choose **Config > Global > All Resource Classes** to add, view, modify, audit, or delete global resource classes.

Related Topics

- Using Resource Classes, page 5-41
- Resource Allocation Constraints, page 5-42
- Using Global Resource Classes, page 5-44
- Using Local Resource Classes, page 5-49
- Auditing Resource Classes, page 5-47

Resource Allocation Constraints

The following resources are critical for maintaining connectivity to the Admin context:

- Rate Bandwidth
- Rate Management Traffic
- Rate SSL Connections
- Rate Connections
- Management Connections
- Concurrent Connections

Caution If you allocate 100 percent of these resources to a resource class and then apply the resource class to virtual contexts, connectivity to the Admin context can be lost.

We recommend that you create a resource class specifically for the Admin context and apply it to the context so that you can maintain IP connectivity.

Table 5-9 Resource Class Attributes

Resource	Definition
Default	Default percentage used for any resource parameter not explicitly set.
Acceleration Connections	Option that is available ACE appliances only. Percentage of application acceleration connections.
ACL Memory	Percentage of memory allocated for ACLs.
Concurrent Connections	Percentage of simultaneous connections. **Note** If you consume all Concurrent Connections by allocating 100 percent to virtual contexts, IP connectivity to the Admin context can be lost.
HTTP Compression	Percentage of compression for HTTP data. **Note** This option appears for ACE appliances.
Management Connections	Percentage of management connections. **Note** If you consume all Management Connections by allocating 100 percent to virtual contexts, IP connectivity to the Admin context can be lost.
Proxy Connections	Percentage of proxy connections.
Regular Expression	Percentage of regular expression memory.
Sticky	Percentage of entries in the sticky table. **Note** You must configure a minimum value for sticky to allocate resources for sticky entries; the sticky software receives no resources under the unlimited setting.
Xlates	Percentage of network and port address translations entries.
Buffer Syslog	Percentage of the syslog buffer.
Rate Inspect Connection	Percentage of application protocol inspection connections.
Rate Bandwidth	Percentage of context throughput. This attribute limits the total ACE throughput in bytes per second for one or more contexts. **Note** If you consume all Rate Bandwidth by allocating 100 percent to virtual contexts, IP connectivity to the Admin context can be lost. The maximum bandwidth rate per context is determined by your ACE bandwidth license.
Rate Connections	Percentage of connections of any kind. **Note** If you consume all Rate Connections by allocating 100 percent to virtual contexts, IP connectivity to the Admin context can be lost.
Rate Management Traffic	Percentage of management traffic connections. **Note** If you consume all Rate Management Traffic by allocating 100 percent to virtual contexts, IP connectivity to the Admin context can be lost.

Table 5-9 Resource Class Attributes (continued)

Resource	Definition
Rate SSL Connections	Percentage of SSL connections. **Note** If you consume all Rate SSL Connections by allocating 100percent to virtual contexts, IP connectivity to the Admin context can be lost.
Rate Syslog	Percentage of syslog messages per second.
Rate MAC Miss	Percentage of messages destined for the ACE that are sent to the control plane when the encapsulation is not correct in packets.

Related Topics

- Using Global Resource Classes, page 5-44
- Configuring Global Resource Classes, page 5-44
- Configuring Local Resource Classes, page 5-50
- Auditing Resource Classes, page 5-47
- Deploying Global Resource Classes, page 5-46

Using Global Resource Classes

Resource classes are used when provisioning services, establishing virtual contexts, managing devices, and monitoring virtual context resource consumption.

Defining a new global resource class does not automatically update all configurations. A global resource class is applied only when the resource class is deployed to a specific Admin virtual context on an ACE.

This section includes the following topics:

- Configuring Global Resource Classes, page 5-44
- Deploying Global Resource Classes, page 5-46
- Auditing Resource Classes, page 5-47
- Modifying Global Resource Classes, page 5-48
- Deleting Global Resource Classes, page 5-49

Configuring Global Resource Classes

You can create a new global resource class and optionally deploy it on an ACE by using the Admin virtual context.

⚠ **Caution** If you allocate 100 percent of these resources to a resource class and then apply the resource class to virtual contexts, connectivity to the Admin context can be lost. For more information, see the "Resource Allocation Constraints" section on page 5-42.

Procedure

Step 1 Choose **Config > Global > All Resource Classes**.

The Resource Classes table appears.

Step 2 In the Resource Classes table, click **Add** to create a new resource class.

The New Resource Class configuration window appears.

Step 3 In the Name field of the New Resource Class configuration window, enter a unique name for this resource class.

Valid entries are unquoted text strings with no spaces and a maximum of 64 characters.

Step 4 In the Description field, enter a brief description for this resource class.

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

Step 5 To use the same values for each resource, in the All row, enter the following information (see Table 5-9 for a description of the resources):

a. In the Min. field, enter the minimum percentage of each resource that you want to allocate to this resource class. Valid entries are numbers from 0 to 100 including those numbers with decimals.

b. In the Max. field, choose the maximum percentage of each resource that you want to allocate to this resource class as follows:

   - Equal To Min—The maximum percentage allocated for each resource is equal to the minimum specified in the Min. field.
   - Unlimited—There is no upper limit on the percentage of each resource that can be allocated for this resource class.

Step 6 To use different values for the resources, for each resource, choose the method for allocating resources:

- Choose **Default** to use the values specified in Step 5.
- Choose **Min** to enter a specific minimum value for the resource.

Step 7 If you chose Min, do the following:

a. In the Min. field, enter the minimum percentage of this resource you want to allocate to this resource class. For example, for ACL memory, enter **10** in the Min. field to indicate that you want to allocate a minimum of 10 percentage of the available ACL memory to this resource class.

b. In the Max. field, choose the maximum percentage of the resource that you want to allocate to this resource class:

   - Equal To Min—The maximum percentage allocated for this resource is equal to the minimum specified in the Min. field.
   - Unlimited—There is no upper limit on the percentage of the resource that can be allocated for this resource class.

Step 8 To deploy the resource class to an Admin context, do the following:

a. Click **Admin VCs To Deploy To** to expand the configuration subset.

b. In the Available Items list, choose the desired Admin context, and click **Add**. The items appear in the Selected Items list.

   In the Selected Items list, choose a context to remove and click **Remove**. The items appear in the Available Items list.

Step 9 Do one of the following:

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

- Click **Cancel** to exit this procedure without saving your entries and to return to the Resource Classes table.

Related Topics

- Using Resource Classes, page 5-41
- Modifying Global Resource Classes, page 5-48
- Deleting Global Resource Classes, page 5-49
- Auditing Resource Classes, page 5-47

Deploying Global Resource Classes

You can apply a global resource class to Admin contexts on selected ACE devices. If you deploy a global resource class to an ACE that already has a resource class with the same name, ANM replaces the properties of the local resource class with the properties from the global resource class. If you deploy a global resource class to an ACE that does not have a resource class with the same name, ANM creates a new local resource class with the same name and properties as the global resource class.

Assumptions

This topic assumes the following:

- At least one global resource class exists.
- At least one ACE has been imported into the ANM.

Procedure

Step 1 Choose **Config > Global > All Resource Classes**.

The Resource Classes table appears.

Step 2 In the Resource Classes table, choose the global resource class that you want to apply to an ACE, and click **Edit**.

The Edit Resource Class configuration window appears.

Step 3 In the Available Items list of the Edit Resource Class configuration window, choose the context that you want to apply this global resource class to, and click **Add**.

The item appears in the Selected Items list.

To remove contexts, choose them in the Selected Items list, and click **Remove**. The items appear in the Available Items list.

Step 4 Do one of the following:

- Click **OK** to save your entries and to return to the Resource Classes table. The context is updated with the resource class configuration.
- Click **Cancel** to exit this procedure without saving your entries and to return to the Resource Classes table.

Related Topics

- Using Resource Classes, page 5-41
- Modifying Global Resource Classes, page 5-48
- Using Local Resource Classes, page 5-49
- Configuring Local Resource Classes, page 5-50

Auditing Resource Classes

You can display any discrepancies that exist between the global resource class and the local resource class on the context after you apply a global resource class to an Admin context. Discrepancies occur when either global or context resource class attributes are modified independently of one another after the global resource class has been applied.

Procedure

Step 1 Choose **Config > Global > All Resource Classes**.

The Resource Classes table appears.

Step 2 In the Resource Classes table, choose the resource class that you want to audit, and click **Audit**.

ANM identifies the differences between the selected resource class and the Admin contexts being managed by ANM and displays the results in the Audit Differences table in a separate window. The table uses the following conventions:

- If the selected resource class has not been applied to an Admin context, the Admin context is listed with the comment "Resource class not defined."
- If the selected resource class has been applied to an Admin context, but there are no differences between the global and local resource classes, the context does not appear in the table.
- If the selected resource class has been applied to an Admin context and there are differences between the global and local resource classes, the context appears in the table with the following information:
  - The resource attribute that has different values in the global and local resource classes.
  - The settings for the resource attribute in the local resource class.
  - The settings for the resource attribute in the global resource class.

  The values displayed use the format *min* - *max* where *min* represents the minimum percentage configured for this attribute and *max* represents the maximum percentage configured for this attribute, such as 8% - 8% or 5% - 100%.

Step 3 Do one of the following:

- Click **Close** to close this window and return to the Resource Classes table.
- Click **Refresh** to update the information in the Audit Differences table.

Related Topics

- Using Global Resource Classes, page 5-44
- Using Local Resource Classes, page 5-49
- Configuring Global Resource Classes, page 5-44

- Configuring Local Resource Classes, page 5-50

Modifying Global Resource Classes

You can modify an existing global resource class. The changes are not applied to virtual contexts previously associated with the resource class. ANM only applies updated resource class properties to virtual contexts that are associated with the resource class going forward.

Caution If you allocate 100 percent of these resources to a resource class and then apply the resource class to virtual contexts, connectivity to the Admin context can be lost. For more information, see the "Resource Allocation Constraints" section on page 5-42.

Procedure

Step 1 Choose **Config > Global > All Resource Classes**.

The Resource Classes table appears.

Step 2 Choose the resource class that you want to modify, and click **Edit**.

The Edit Resource Class configuration window appears.

Step 3 In the Edit Resource Class configuration window, modify the values as desired.

For details on setting values, see the "Configuring Global Resource Classes" section on page 5-44. For descriptions of the resources, see Table 5-9.

Step 4 To deploy the modified resource class to an Admin context, do the following:

a. Click **Admin VCs To Deploy To** to expand the configuration subset.

b. Choose the desired context in the Available Items list, and click **Add**. The item appears in the Selected Items list.

Note ANM only applies the updated resource class to contexts that you choose and add to the Selected Items list. It does not apply the modified resource class to contexts previously associated with the resource class.

Step 5 Do one of the following:

- Click **OK** to save your entries, apply them to the selected contexts, and return to the Resource Classes table.
- Click **Cancel** to exit this procedure without saving your entries and to return to the Resource Classes table.

Related Topics

- Using Resource Classes, page 5-41
- Using Global Resource Classes, page 5-44
- Modifying Global Resource Classes, page 5-48
- Auditing Resource Classes, page 5-47

- Deleting Global Resource Classes, page 5-49

Deleting Global Resource Classes

You can remove global resource classes from the ANM database. Because global resource classes are managed separately from local resource classes, deleting a global resource class does not affect local resource classes deployed on individual contexts.

Procedure

Step 1 Choose **Config > Global > All Resource Classes**.

The Resource Classes table appears.

Step 2 In the Resource Classes table, choose the resource class that you want to remove, and click **Delete**.

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

Step 3 Click **OK** to delete the resource class or **Cancel** to retain the resource class.

The Resource Classes table refreshes with the updated information.

Related Topics

- Using Resource Classes, page 5-41
- Using Global Resource Classes, page 5-44
- Modifying Global Resource Classes, page 5-48
- Auditing Resource Classes, page 5-47

Using Local Resource Classes

You can create local resource classes in ANM as follows:

- During the import process, from any ACE with a previously configured resource class. These resource classes appear in the ANM in the Admin virtual context associated with the imported ACE.
- By an Admin user in ANM using the local Resource Class configuration option (Config > Devices > Admin_context > System > Resource Classes).
- By creating a global resource class (Config > Global > All Resource Classes) and applying it to an Admin context.

Note Local resource class configuration options are available in Admin contexts only.

This section includes the following topics:

- Configuring Local Resource Classes, page 5-50
- Deleting Local Resource Classes, page 5-51
- Displaying Local Resource Class Use on Virtual Contexts, page 5-52

Configuring Local Resource Classes

Note This functionality is available in Admin contexts only.

You can create or modify a local resource class for use within the selected Admin context.

Procedure

Step 1 Choose **Config** > **Devices** > *Admin_context* > **System** > **Resource Classes**.

The Resource Classes table appears.

Step 2 In the Resource Classes table, click **Add** to create a new local resource class or choose an existing resource class, and click **Edit** to modify it.

The Resource Class configuration window appears.

Step 3 In the Name field of the Resource Class configuration window, enter a unique name for this resource class.

Valid entries are unquoted text strings with no spaces and a maximum of 64 characters.

Step 4 To use the same values for each resource, in the All row, enter the following information (see Table 5-9 for a description of the resources):

a. In the Min. field, enter the minimum percentage of each resource that you want to allocate to this resource class. Valid entries are numbers from 0 to 100 including those numbers with decimals.

b. In the Max. field, choose the maximum percentage of each resource that you want to allocate to this resource class:

   - Equal To Min—The maximum percentage allocated for each resource is equal to the minimum specified in the Min. field.
   - Unlimited—There is no upper limit on the percentage of each resource that can be allocated for this resource class.

Step 5 To use different values for the resources, for each resource, choose one of the following methods for allocating resources:

- Choose **Default** to use the values specified in Step 5.
- Choose **Min** to enter a specific minimum value for the resource.

Step 6 (Optional) If you chose Min, do the following:

a. In the Min. field, enter the minimum percentage of this resource you want to allocate to this resource class. For example, for ACL memory, enter **10** in the Min. field to indicate that you want to allocate a minimum of 10 percent of the available ACL memory to this resource class.

b. In the Max. field, choose the maximum percentage of the resource that you want to allocate to this resource class:

   - **Equal To Min**—The maximum percentage allocated for this resource is equal to the minimum specified in the Min. field.
   - **Unlimited**—There is no upper limit on the percentage of the resource that can be allocated for this resource class.

Step 7 When you finish allocating resources for this resource class, do one of the following:

- Click **OK** to save your entries and to return to the Resource Classes table. The resource class can now be applied to other virtual contexts on the same ACE.
- Click **Cancel** to exit this procedure without saving your entries and to return to the Resource Classes table.

Related Topics

- Using Resource Classes, page 5-41
- Using Local Resource Classes, page 5-49
- Displaying Local Resource Class Use on Virtual Contexts, page 5-52
- Deleting Local Resource Classes, page 5-51

Deleting Local Resource Classes

You can delete a local resource class. Because of the possible impact on virtual contexts of deleting a local resource class, you cannot delete a resource class that is associated with a virtual context. To display a resource class's current deployment, see the "Displaying Local Resource Class Use on Virtual Contexts" section on page 5-52.

Procedure

Step 1 Choose **Config > Devices >** *Admin_context* **> System > Resource Classes**.

The Resource Classes table lists all local resource classes and the number of virtual contexts using each resource class.

Step 2 Confirm that the resource class that you want to delete is not deployed on any virtual contexts.

You cannot delete a resource class that is deployed on a context.

To identify the contexts using a specific resource class, see the "Displaying Local Resource Class Use on Virtual Contexts" section on page 5-52.

Step 3 Choose the resource class that you want to remove, and click **Delete**.

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

Step 4 Click **OK** to delete the resource class or **Cancel** to retain the resource class.

The Resource Classes table refreshes with the updated information.

Related Topics

- Using Resource Classes, page 5-41
- Configuring Local Resource Classes, page 5-50
- Displaying Local Resource Class Use on Virtual Contexts, page 5-52

Displaying Local Resource Class Use on Virtual Contexts

You can display local resource class usage on all virtual contexts on an ACE.

Procedure

Step 1 Choose **Config > Devices**.

The device tree appears.

Step 2 In the device tree, choose the ACE with the resource class usage that you want to display.

The Virtual Contexts table appears, listing all contexts on the selected ACE and the resource class in use for each context.

Step 3 (Optional) In the Virtual Contexts table, click the Resource Class column heading to sort the table by resource class.

Related Topics

- Using Resource Classes, page 5-41
- Configuring Local Resource Classes, page 5-50
- Deleting Local Resource Classes, page 5-51

Using the Configuration Checkpoint and Rollback Service

At some point, you may want to modify your ACE running configuration. If you run into a problem with the modified configuration, you may need to reboot your ACE. To prevent having to reboot your ACE after unsuccessfully modifying a running configuration, you can create a checkpoint (a snapshot in time) of a known stable running configuration before you begin to modify it. If you encounter a problem with the modifications to the running configuration, you can roll back the configuration to the previous stable configuration checkpoint.

Note Before you upgrade your ACE software, we strongly recommend that you create a checkpoint in your running configuration. For ACE module A2(3.0) and later releases only, use the backup function to create a backup of the running configuration (see the "Performing Device Backup and Restore Functions" section on page 5-56).

The ACE allows you to make a checkpoint configuration at the context level. The ACE stores the checkpoint for each context in a hidden directory in Flash memory. If, after you make configuration changes that modify the current running configuration, when you roll back the checkpoint, the ACE causes the running configuration to revert to the checkpointed configuration.

This section includes the following topics:

- Creating a Configuration Checkpoint, page 5-53
- Deleting a Configuration Checkpoint, page 5-54
- Rolling Back a Running Configuration, page 5-54
- Displaying Checkpoint Information, page 5-54

Creating a Configuration Checkpoint

You can create a configuration checkpoint for a specific context. The ACE supports a maximum of 10 checkpoints for each context.

Assumption

This topic assumes the following:

- Make sure that the current running configuration is stable and is the configuration that you want to make as a checkpoint. If you change your mind after creating the checkpoint, you can delete it (see the "Deleting a Configuration Checkpoint" section on page 5-54).
- The ACE-Admin, ANM-Admin, and Org-Admin predefined roles have access to the configuration checkpoint function.
- A custom role defined with the task ANM Inventory > Virtual Context/Create or ANM Inventory > Virtual Context/Modify has the required privileges to create a configuration checkpoint.
- A checkpoint will not include the SSL keys/certificates, probe scripts, and licenses.
- Adding a checkpoint from an ACE context directly will not trigger an autosynchronzation on ANM for that context.

Procedure

Step 1 Choose **Config > Devices >** *context* > **System > Checkpoints**.

The Checkpoints table appears.

For descriptions of the checkpoints, see Table 5-10.

Table 5-10 Checkpoints Table

Field	Description
Name	Unique identifier of the checkpoint.
Size (In Bytes)	Size of the configuration checkpoint, shown in bytes.
Date (Created On)	Date that the configuration checkpoint was created.

Step 2 In the Checkpoints table, click the **Create Checkpoint** button.

The Create Checkpoint dialog box appears.

Step 3 In the Checkpoint Name field of the Create Checkpoint dialog box, specify a unique identifier for the checkpoint.

Enter a text string with no spaces and a maximum of 25 alphanumeric characters.

If the checkpoint already exists, you are prompted to use a different name.

Step 4 Do one of the following:

- Click **OK** to save your configuration checkpoint. You return to the Checkpoints table and the new checkpoint appears in the table.
- Click **Cancel** to exit the procedure without saving the configuration checkpoint and to return to the Checkpoints table.

Deleting a Configuration Checkpoint

You can delete a checkpoint. Deleting a checkpoint from an ACE context directly will not trigger an autosynchronzation to occur on ANM for that context.

Prerequisite

Before you perform this procedure, make sure that you want to delete the checkpoint. Once you click the Trash icon, the ACE removes the checkpoint from Flash memory.

Procedure

Step 1 To choose a virtual context that you want to create a configuration checkpoint, choose **Config > Devices >** *context* > **System > Checkpoints**.

The Checkpoints table appears.

Step 2 In the Checkpoints table, choose the radio button to the left of any table entry, and click the **Trash** icon to delete the checkpoint.

Rolling Back a Running Configuration

You can roll back the current running configuration of a context to the previously checkpointed running configuration.

Procedure

Step 1 Choose **Config > Devices >** *context* > **System > Checkpoints**.

The Checkpoints table appears.

Step 2 Choose the radio button to the left of the checkpoint that you wish to roll back, and click **Rollback**.

ANM displays a confirmation popup window to warn you about this change and to instruct you that the rollback operation may take longer depending on the differences detected between the two configurations.

Note ANM synchronizes the device after performing a rollback. This synchronzation may take some time.

Displaying Checkpoint Information

You can display checkpoint information.

Procedure

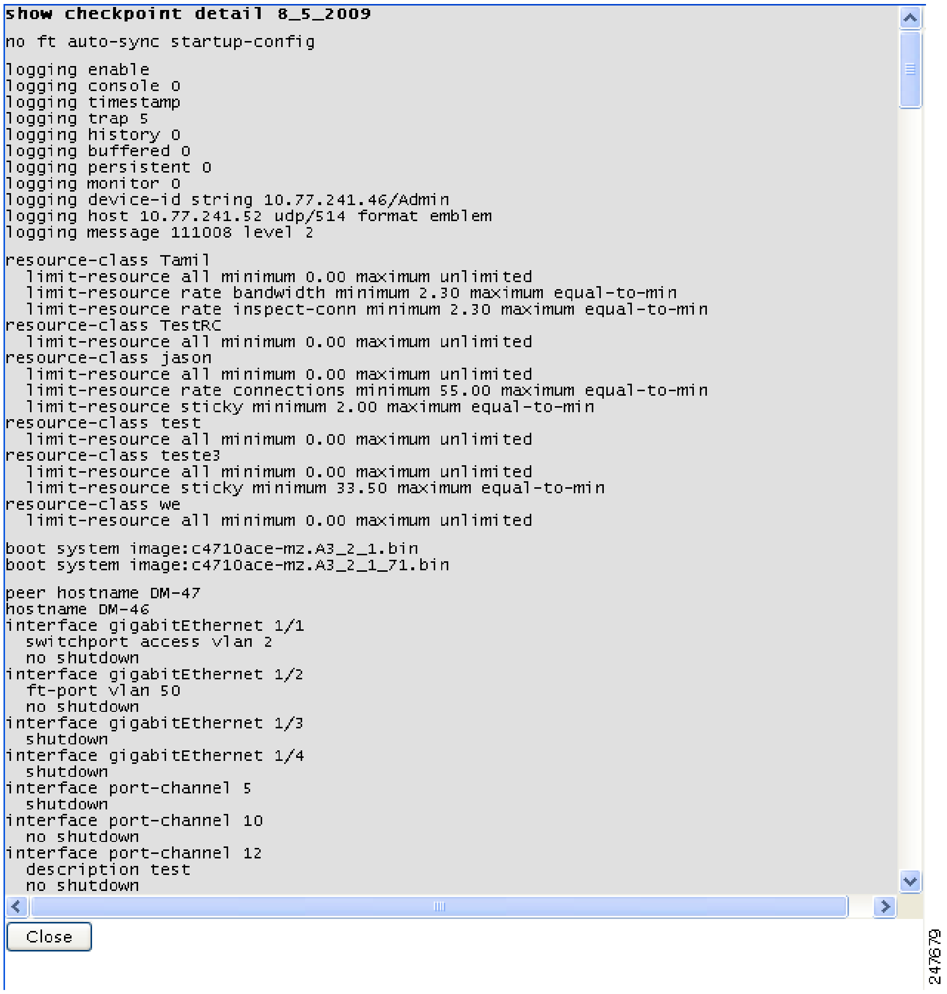
Step 1 Choose **Config > Devices >** *context* > **System > Checkpoints**.

The Checkpoints table appears.

Step 2 In the Checkpoints table, choose the radio button to the left of the checkpoint that you want to display, and click **Details**.

ANM uses the ACE **show checkpoint detail** {*name*} CLI command to display the running configuration of the specified checkpoint (see Figure 5-1).

Figure 5-1 show checkpoint detail CLI Command Dialog Box



```
show checkpoint detail 8_5_2009
no ft auto-sync startup-config

logging enable
logging console 0
logging timestamp
logging trap 5
logging history 0
logging buffered 0
logging persistent 0
logging monitor 0
logging device-id string 10.77.241.46/Admin
logging host 10.77.241.52 udp/514 format emblem
logging message 111008 level 2

resource-class Tamil
  limit-resource all minimum 0.00 maximum unlimited
  limit-resource rate bandwidth minimum 2.30 maximum equal-to-min
  limit-resource rate inspect-conn minimum 2.30 maximum equal-to-min
resource-class TestRC
  limit-resource all minimum 0.00 maximum unlimited
resource-class jason
  limit-resource all minimum 0.00 maximum unlimited
  limit-resource rate connections minimum 55.00 maximum equal-to-min
  limit-resource sticky minimum 2.00 maximum equal-to-min
resource-class test
  limit-resource all minimum 0.00 maximum unlimited
resource-class teste3
  limit-resource all minimum 0.00 maximum unlimited
  limit-resource sticky minimum 33.50 maximum equal-to-min
resource-class we
  limit-resource all minimum 0.00 maximum unlimited

boot system image:c4710ace-mz.A3_2_1.bin
boot system image:c4710ace-mz.A3_2_1_71.bin

peer hostname DM-47
hostname DM-46
interface gigabitEthernet 1/1
  switchport access vlan 2
  no shutdown
interface gigabitEthernet 1/2
  ft-port vlan 50
  no shutdown
interface gigabitEthernet 1/3
  shutdown
interface gigabitEthernet 1/4
  shutdown
interface port-channel 5
  shutdown
interface port-channel 10
  no shutdown
interface port-channel 12
  description test
  no shutdown
```

Step 3 Click **Close** to exit the dialog box and return to the Checkpoints table.

Performing Device Backup and Restore Functions

Note The backup and restore functions are available for the ACE module A2(3.0) and later releases only.

The backup and restore functions allow you to back up or restore the configuration and dependencies of an entire ACE or of a particular virtual context. Configuration dependencies are those files that are required to exist on the ACE so that a configuration can be applied to it. Such files include health-monitoring scripts, SSL certificates, SSL keys, and so on.This feature allows you to back up and restore the following configuration files and dependencies:

- Running-configuration files
- Startup-configuration files
- Checkpoints
- SSL files (SSL certificates and keys)
- Health-monitoring scripts
- Licenses

Note The backup feature does not back up the sample SSL certificate and key pair files.

Typical uses for this feature are as follows:

- Back up a configuration for later use
- Recover a configuration that was lost because of a software failure or user error
- Restore configuration files to a new ACE when a hardware failure resulted in a Return Merchandise Authorization (RMA) of the old ACE
- Transfer the configuration files to a different ACE

The backup and restore functions are supported in both the Admin and virtual contexts. If you perform these functions in the Admin context, you can back up or restore the configuration files for either the Admin context only or for all contexts in the ACE. If you perform these functions in a virtual context, you can back up or restore the configuration files only for that context. Both the backup and the restore functions run asynchronously (in the background).

Note To perform the back up or copy functions on multiple ACEs simultaneously, see the "Performing Global Device Backup and Copy Functions" section on page 5-64

Archive Naming Conventions

Context archive files have the following naming convention format:

Hostname_ctxname_timestamp.tgz

The filename fields are as follows:

– *Hostname*—Name of the ACE. If the hostname contains special characters, the ACE uses the default hostname "switch" in the filename. For example, if the hostname is Active@~!#$%^, then the ACE assigns the following filename: switch_Admin_2009_08_30_15_45_17.tgz

- *ctxname*—Name of the context. If the context name contains special characters, the ACE uses the default context name "context" in the filename. For example, if the context name is Test!123*, then the ACE assigns the following filename: switch_context_2009_08_30_15_45_17.tgz
- *timestamp*—Date and time that the ACE created the file. The time stamp has the following 24 hour format: *YYYY_MM_DD_hh_mm_ss*

An example is as follows:

```
ACE-1_ctx1_2009_05_06_15_24_57.tgz
```

If you back up the entire ACE, the archive filename does not include the *ctxname* field. So, the format is as follows:

Hostname_timestamp.tgz

An example is as follows:

```
ACE-1_2009_05_06_15_24_57.tgz
```

Archive Directory Structure and Filenames

The ACE uses a flat directory structure for the backup archive. The ACE provides file extensions for the individual files that it backs up so that you can identify the types of files easily when restoring an archive. All files are stored in a single directory that is tarred and GZIPed as follows:

```
ACE-1_Ctx1_2009_05_06_07_24_57.tgz
 ACE-1_Ctx1_2009_05_06_07_24_57\
  context_name-running
  context_name-startup
  context_name-chkpt_name.chkpt
  context_name-cert_name.cert
  context_name-key_name.key
  context_name-script_name.tcl
  context_name-license_name.lic
```

Guidelines and Limitations

The backup and restore functions have the following configuration guidelines and limitations:

- Store the backup archive on disk0: in the context of the ACE where you intend to restore the files. Use the Admin context for a full backup and the corresponding context for user contexts.
- When you back up the running-configuration file, the ACE uses the output of the **show running-configuration** CLI command as the basis for the archive file.
- The ACE backs up only exportable certificates and keys.
- License files are backed up only when you back up the Admin context.
- Use a pass phrase to back up SSL keys in encrypted form. Remember the pass phrase or write it down and store it in a safe location. When you restore the encrypted keys, the ACE prompts you for the pass phrase to decrypt the keys. If you do not use a pass phrase when you back up the SSL keys, the ACE restores the keys with AES-256 encryption using OpenSSL software.
- Only probe scripts that reside in disk0: need to be backed up. The prepackaged probe scripts in the probe: directory are always available. When you perform a backup, the ACE automatically identifies and backs up the scripts in disk0: that are required by the configuration.
- The ACE does not resolve any other dependencies required by the configuration during a backup except for scripts that reside in disk0:. For example, if you configured SSL certificates in an SSL proxy in the running-configuration file, but you later deleted the certificates, the backup proceeds anyway as if the certificates still existed.

- To perform a restore operation, you must have the admin RBAC feature in your user role. ANM-admin and ORG-admin have access to this feature by default. Custom roles with the ANM Inventory and Virtual Context role tasks set to create or modify can also access this feature.
- When you instruct the ACE to restore the archive for the entire ACE, it restores the Admin context completely first, and then it restores the other contexts. The ACE restores all dependencies before it restores the running configuration. The order in which the ACE restores dependencies is as follows:
  - License files
  - SSL certificates and key files
  - Health-monitoring scripts
  - Checkpoints
  - Startup-configuration file
  - Running-configuration file
- When you restore the ACE, previously installed license files are uninstalled and the license files in the backup file are installed in their place.
- In a redundant configuration, if the archive that you want to restore is different from the peer configurations in the FT group, redundancy may not operate properly after the restore.
- You can restore a single context from a full backup archive provided that:
  - You execute the restore operation in the context that you want to restore
  - All files dependencies for the context exist in the full backup archive
- To enable ANM to synchronize the CLI after a successful restore, do not navigate from the Backup / Restore page until the Latest Restore status changes from In Progress to Success. If you navigate to another page before the restore process is complete, the CLI will not synchronize until you return to the Backup / Restore page.

Defaults

Table 5-11 lists the default settings for the backup and restore function parameters.

Table 5-11 Default Backup and Restore Parameters

Parameter	Default
Backed up files	By default the ACE backs up the following files in the current context: • Running-configuration file • Startup-configuration file • Checkpoints • SSL certificates • SSL keys • Health-monitoring scripts • Licenses
SSL key restore encryption	None

This section includes the following topics:

- Backing Up Device Configuration and Dependencies, page 5-59

- Restoring Device Configuration and Dependencies, page 5-62

Backing Up Device Configuration and Dependencies

You can create a backup of an ACE configuration and its dependencies.

Note When you perform the backup process from the Admin context, you can either back up the Admin context files only or you can back up the Admin context and all user contexts. When you back up from a user context, you back up the current context files only and cannot back up the ACE licenses.

Note If your web browser supports the Remember Passwords option and you enable this option, the web browser may fill in the Username and Password fields for user authentication. By default, these fields should be empty. You can change the username and password fields from whatever the web browser inserts into the two fields.

Procedure

Step 1 Choose **Config > Devices >** *context* > **System > Backup / Restore**.

The Backup / Restore table appears and displays the latest backup and restore statistics.

Note To refresh the table content at any time, click **Poll Now**.

Note When you choose the Backup / Restore operation, ANM must poll a context if that context has not been accessed previously for this operation. The polling operation, which is necessary to obtain the latest backup and restore information, can cause a delay in the display time of the Backup / Restore table.

The Backup / Restore fields are described in Table 5-12.

Table 5-12 Backup / Restore Fields

Field	Description
Latest Backup	
Backup Archive	Name of the last *.tgz file created that contains the backup files.
Type	Type of backup: Context or Full (all contexts).
Start-time	Date and time that the last backup began.
Finished-time	Date and time that the last backup ended.
Status	Status of the last context to be backed up: Success, In Progress, or Failed. Click the status link to view status details.
Current vc	Name of the last context in the backup process.

Table 5-12 Backup / Restore Fields (continued)

Field	Description
Completed	Number of context backups completed compared to the total number of context backup requests. For example: • 2/2 = Two context backups completed/Two context backups requested • 0/1 = No context backup completed/One context backup requested
Latest Restore	
Backup Archive	Name of the *.tgz file used in during the restore process.
Type	Type of restore: Context or Full (all contexts).
Start-time	Date and time that the last restore began.
Finished-time	Date and time that the last restore ended.
Status	Status of the last restore: Success, In Progress, or Failed. Click the status to view status details.
Current vc	Name of the last context in the restore process.
Completed	Number of context restores completed compared to the total number of context restore requests. For example: • 2/2 = Two context restores completed/Two context restores requested • 0/1 = No context restore completed/One context restore requested

Step 2 Click **Backup**.

The Backup window appears.

Step 3 In the Backup window, click the radio button of the location where the ACE is to save the backup files:

- **Backup config on ACE (disk0:)**—This is the default. Go to Step 9.
- **Backup config on ACE (disk0:) and then copy to remote system**—The Remote System attributes step appears. Go to Step 4.

Step 4 Click the radio button of the transfer protocol to use:

- **FTP**—File Transfer Protocol
- **SFTP**—Secure File Transfer Protocol
- **TFTP**—Trivial File Transfer Protocol

Step 5 In the Username field, enter the username that the remote server requires for user authentication.

This field appears for FTP and SFTP only.

Step 6 In the Password field, enter the password that the remote server requires for user authentication.

This field appears for FTP and SFTP only.

Step 7 In the IP Address field, enter the IP address of the remote server.

Step 8 In the Backup File Path in Remote System field, enter the full path for the remote server.

Step 9 Check the **Backup All Contexts** checkbox if you want the ACE to create a backup that contains the files of the Admin context and every user context or uncheck the check box to create a backup of the Admin context files only.

This field appears for the Admin context only.

Step 10 Indicate the components to exclude from the backup process: Checkpoints or SSL Files.

To exclude a component, double-click on it in the Available box to move it to the Selected box. You can also use the right and left arrows to move selected items between the two boxes.

Caution If you exclude the SSL Files component and then restore the ACE using this archived backup, these files are removed from the ACE. To save these files prior to performing a restore with this backup, use the **crypto export** CLI command to export the keys to a remote server and use the **copy** CLI command to copy the license files to disk0: as .tar files.

Step 11 In the Pass Phrase field, enter the pass phrase that you specify to encrypt the backed up SSL keys.

Enter the pass phrase as an unquoted text string with no spaces and a maximum of 40 alphanumeric characters. If you enter a pass phrase but exclude the SSL files from the archive, the ACE does not use the pass phrase.

Step 12 Click **OK** to begin the backup process.

The following actions occur depending on where ANM saves the files:

- disk0: only—ANM permits continued GUI functionality during the backup process and polls the ACE for the backup status, which it displays on the Backup / Restore page.
- disk0: and a remote server— ANM suspends GUI operation and displays a “Please Wait” message in the Backup dialog box until the process is complete. During this process, ANM instructs the ACE to create and save the backup file locally to disk0: and then place a copy of the file on the specified remote server.

Step 13 In the Backup / Restore page, click **Poll Now** or click the browser refresh button to ensure that the latest backup statistics are displayed, and then click on the Status link (**Success**, **In Progress**, or **Failed**) located in the Latest Backup column to view details of the backup operation.

If the backup status is either Success or In Progress, then the Show Backup Status Detail pop-up window appears and displays a list of the files successfully backed up. When the backup status is In Progress, ANM polls the ACE every 2 minutes to retrieve the latest status information and then it automatically updates the status information displayed. The polling continues until ANM receives a status of either Success or Failed. If the backup status is Failed, then the Show Backup Errors popup window appears, displaying the reason for the failed backup attempt.

Related Topics

- Restoring Device Configuration and Dependencies, page 5-62
- Performing Global Device Backup and Copy Functions, page 5-64

Restoring Device Configuration and Dependencies

You can restore an ACE configuration and its dependencies using a backup file.

Caution The restore operation clears any existing SSL certificate and key-pair files, license files, and checkpoints in a context before it restores the backup archive file. If your configuration includes SSL files or checkpoints and you excluded them when you created the backup archive, those files will no longer exist in the context after you restore the backup archive. To preserve any existing exportable SSL certificate and key files in the context, before you execute the restore operation, export the certificates and keys that you want to keep to an FTP, SFTP, or TFTP server by using the CLI and the **crypto export** command. After you restore the archive, import the SSL files into the context. For details on exporting and importing SSL certificate and key pair files using the CLI, see the *Cisco Application Control Engine Module SSL Configuration Guide*.

You can also use the exclude option of the restore command to instruct the ACE not to clear the SSL files in disk0: and to ignore the SSL files in the backup archive when the ACE restores the backup.

Note If your web browser supports the Remember Passwords option and you enable this option, the web browser may fill in the Username and Password fields for user authentication. By default, these fields should be empty. You can change the username and password fields from whatever the web browser inserts into the two fields.

Prerequisites

If you are going to restore the Admin context files plus all user context files, use a backup file that was created from the Admin context with the Backup All Contexts checkbox checked (see the "Backing Up Device Configuration and Dependencies" section on page 5-59).

Procedure

Step 1 Choose **Config > Devices >** *context* > **System > Backup / Restore**.

The Backup / Restore table appears.

Note To refresh the table content at any time, click **Poll Now**.

Note When you perform the restore process from the Admin context, you can either restore the Admin context files only or you can restore the Admin context files plus all user context files. When you perform the restore process from a user context, you can restore the current context files only.

The Backup / Restore fields are described in Table 5-12.

Step 2 Click **Restore**.

The Restore window appears.

Step 3 In the Restore window, click the desired radio button to specify the location where the backup files are located saved:

- **Choose a backup file on the ACE (disk0:)**—This is the default. Go to Step 9.
- **Choose a backup file from remote system**—The Remote System attributes step appears. Go to Step 4.

Step 4 Click the radio button of the transfer protocol to use:

- **FTP**—File Transfer Protocol
- **SFTP**—Secure File Transfer Protocol
- **TFTP**—Trivial File Transfer Protocol

Step 5 In the Username field, enter the username that the remote file system requires for user authentication.

This field appears for FTP and SFTP only.

Step 6 In the Password field, enter the password that the remote file system requires for user authentication.

This field appears for FTP and SFTP only.

Step 7 In the IP Address field, enter the IP address of the remote server.

Step 8 In the Backup File Path in Remote System field, enter the full path of the backup file, including the backup filename, to be copied from the remote server.

Step 9 Check the **Restore All Contexts** checkbox if you want the ACE to restore the files for every context or uncheck the checkbox to restore the Admin context files only.

This field appears for the Admin context only.

Step 10 Check the **Exclude SSL Files** checkbox if you want to preserver the SSL files currently loaded on the ACE and not use the backup file's SSL files.

Caution The restore function deletes all SSL files currently loaded on the ACE unless you check the Exclude SSL Files option. If you do not check this option, the restore functions loads the SSL files included in the backup file. If the backup files does not include SSL files, the ACE will not have any SSL files loaded on it when the restore process is complete. You will then need to import copies of the SSL files from a remote server.

Step 11 In the Pass Phrase field, enter the pass phrase that is used to encrypt the backed up SSL keys in the archive.

Enter the pass phrase as an unquoted text string with no spaces and a maximum of 40 alphanumeric characters. The Pass Phrase field does not appear when you check the Exclude SSL Files checkbox.

Step 12 Click **OK** to begin the restore process.

The following actions occur depending on where ANM retrieves the backup files:

- disk0: only—ANM permits continued GUI functionality during the restore process and polls the ACE for the backup status, which it displays on the Backup / Restore page.

Note To enable ANM to synchronize the CLI after a successful restore, do not navigate from the Backup / Restore window until the Latest Restore status changes from In Progress to Success. If you navigate to another window before the restore process is complete, the CLI will not synchronize until you return to the Backup / Restore window.

- disk0: and a remote server— ANM suspends GUI operation and displays a "Please Wait" message in the Restore dialog box until the process is complete. During this process, ANM instructs the ACE to copy the backup file from the specified remote server to disk0: on the ACE and then apply the backup file to the context.

Step 13 In the Backup / Restore page, click **Poll Now** or click the browser refresh button to ensure that the latest restore statistics are displayed, then click on the Status link (**Success**, **In Progress**, or **Failed**) located in the Latest Backup column to view details of the restore operation.

If the restore status is either Success or In Progress, then the Show Restore Status Detail popup window appears and displays a list of the files successfully restored. When the restore status is In Progress, ANM polls the ACE every 2 minutes to retrieve the latest status information and then it automatically updates the status information displayed. The polling continues until ANM receives a status of either Success or Failed. If the restored status is Failed, then the Show Restored Errors popup window appears, displaying the reason for the failed restore attempt.

Related Topics

- Performing Device Backup and Restore Functions, page 5-56
- Performing Global Device Backup and Copy Functions, page 5-64

Performing Global Device Backup and Copy Functions

Note The global backup and copy functions are available for the ACE module A2(3.0) and later releases only.

The global backup and copy functions allow you to either back up the configuration and dependencies of multiple ACEs simultaneously or copy existing backup configuration files from disk0: of multiple ACEs to a remote server. Configuration dependencies are those files that are required to exist on the ACE so that a configuration can be applied to it. Such files include health-monitoring scripts, SSL certificates, SSL keys, and so on. This feature allows you to back up and restore the following configuration files and dependencies:

- License files
- Running-configuration files
- Startup-configuration files
- Checkpoints
- SSL files (SSL certificates and keys)
- Health-monitoring scripts

During the backup, each ACE saves its configuration files locally to disk0: in a single directory that is tarred and GZIPed. For more information about the backup function, including guidelines and restrictions, see the "Performing Device Backup and Restore Functions" section on page 5-56.

This section includes the following topics:

- Backing Up Multiple Device Configuration and SSL Files, page 5-65
- Copying Existing Tarred Backup Files to a Remote Server, page 5-66

Backing Up Multiple Device Configuration and SSL Files

You can back up the configuration and SSL files for multiple ACEs simultaneously.

Note If your web browser supports the Remember Passwords option and you enable this option, the web browser may fill in the Username and Password fields for user authentication. By default, these fields should be empty. You can change the username and password fields from whatever the web browser inserts into the two fields.

Procedure

Step 1 Choose **Config > Global > All Backups**.

The Backups table appears and displays a list of the available ACEs.

Note To refresh the table content at any time, click **Poll Now**.

Note When you choose the All Backups operation, ANM must poll all Admin contexts that have not been accessed previously for this operation. The polling operation, which is necessary to obtain the latest backup and restore information, can cause a delay in the display time of the Backups table.

The Backups fields are described in Table 5-13.

Table 5-13 Backups Fields

Field	Description
Name	Name of the ACE.
Management IPs	Management interface IP addresses. When there are multiple IP addresses, they display as shown in the following example: 10.77.241.18/10.77.241.28/10.77.241.38
Latest Backup Time	Date and time that the last backup occurred.
Latest Backup Status	Status of the last backup attempt: Success, In Progress, or Failed. Click the status link to view status details.
Latest Restore Time	Date and time that the last restore occurred.
Latest Restore Status	Status of the last restore attempt: Success, In Progress, or Failed. Click the status link to view status details.
Last Poll Time	Date and time that ANM last polled the device for backup statistics.

Step 2 In the Backups table, check the checkbox of the ACE or ACEs to back up.

Note To choose all of the ACEs, check the Name checkbox.

Step 3 Click **Backup**.

The Backup on devices dialog box appears.

Step 4 In the Backup on devices dialog box, check the Backup All Contexts checkbox if you want each ACE to create a backup that contains the files of its Admin context and every user context or uncheck the check box to create a backup of the Admin context files only.

Step 5 Indicate the components that you want to exclude from the backup process: Checkpoints or SSL Files.

To exclude a component, click on it in the Available box and then click Add (right arrow) to move it to the Selected box. Use Remove (left arrow) to move items from the Selected back to the Available box if needed.

Caution If you exclude the SSL Files component and then restore the ACE using this archived backup, these files are removed from the ACE. To save these files prior to performing a restore with this backup, use the **crypto export** CLI command to export the keys to a remote server and use the **copy** CLI command to copy the license files to disk0: as .tar files.

Step 6 In the Pass Phrase field, enter the pass phrase that you specify to encrypt the backed up SSL keys.

Enter the pass phrase as an unquoted text string with no spaces and a maximum of 40 alphanumeric characters. If you enter a pass phrase but excluded the SSL files from the archive, the ACE does not use the pass phrase.

Step 7 Click **OK** to begin the backup.

Step 8 In the Backups page, click **Poll Now** or click the browser refresh button to ensure that the latest statistics are displayed, and then click on the Status link (**Success**, **In Progress**, or **Failed**) located in the Latest Backup Status column to view details of the backup.

If the backup status is either Success or In Progress, then the Show Backup Status Detail popup window appears and displays a list of the files successfully backed up. When the backup status is In Progress, ANM polls each ACE every 2 minutes to retrieve the latest status information and then it automatically updates the status information displayed. The polling continues until ANM receives a status of either Success or Failed.

If the backup status is Failed, then the Show Backup Errors popup window appears, displaying the reason for the failed backup attempt.

Related Topics

- Copying Existing Tarred Backup Files to a Remote Server, page 5-66
- Performing Device Backup and Restore Functions, page 5-56

Copying Existing Tarred Backup Files to a Remote Server

You can copy an existing back up file from disk0: to a remote server. During the global backup process, each ACE creates a tarred file containing its backup files and saves it locally on disk0:. You can use ANM to simultaneously copy these tarred files from multiple ACEs to a remote server.

Note If your web browser supports the Remember Passwords option and you enable this option, the web browser may fill in the Username and Password fields for user authentication. By default, these fields should be empty. You can change the username and password fields from whatever the web browser inserts into the two fields.

Procedure

Step 1 Choose **Config > Global > All Backups**.

The Backups table appears and displays a list of the available ACEs.

Note To refresh the table content at any time, click **Poll Now**.

The Backups fields are described in Table 5-13.

Step 2 In the Backups table, check the checkbox of the ACE or ACEs to perform the copy function.

Note To choose all of the ACEs, check the Name checkbox.

Step 3 Click **Copy**.

The Copy backup files to a remote system dialog box appears.

Step 4 In the Copy backup files to a remote system dialog box, choose the backup file to copy from the selected device.

This option appears only when you have selected a specific device for the copy operation in Step 2. If you selected multiple devices in Step 2, then each device copies its latest successful backup file to the remote server.

Step 5 Click the radio button of the transfer protocol to use.

- **FTP**—File Transfer Protocol
- **SFTP**—Secure File Transfer Protocol
- **TFTP**—Trivial File Transfer Protocol

Step 6 In the Username field, enter the username that the remote server requires for user authentication.

This field appears for FTP and SFTP only.

Step 7 In the Password field, enter the password that the remote server requires for user authentication.

This field appears for FTP and SFTP only.

Step 8 In the IP Address field, enter the IP address of the remote server.

Step 9 In the Backup File Path in Remote System field, enter the full path for the remote server.

Step 10 Click **OK** to begin the copy process.

ANM copies the backup files from each device to the remote server. A popup message displays to indicate whether a copy operation was successful or failed.

Related Topics

- Backing Up Multiple Device Configuration and SSL Files, page 5-65
- Performing Device Backup and Restore Functions, page 5-56

Configuring Security with ACLs

An access control list (ACL) consists of a series of statements called ACL entries that collectively define the network traffic profile. Each entry permits or denies network traffic (inbound and outbound) to the parts of your network specified in the entry. In addition to an action element (permit or deny), each entry also contains a filter element based on criteria such as the source address, the destination address, the protocol, or the protocol-specific parameters. An implicit "deny all" entry exists at the end of every ACL, so you must configure an ACL on every interface where you want to permit connections; otherwise, the ACE denies all traffic on the interface.

ACLs provide basic security for your network by allowing you to control network connection setups rather than processing each packet. Such ACLs are commonly referred to as *security ACLs*.

You can configure ACLs as parts of other features; for example, security, network address translation (NAT), or server load balancing (SLB). The ACE merges these individual ACLs into one large ACL called a *merged ACL*. The ACL compiler then parses the merged ACL and generates the ACL lookup mechanisms. A match on this merged ACL can result in multiple actions. You can add, modify, or delete entries to an ACL already in the summary table, or add a new ACL to the list.

When you use ACLs, you may want to permit all e-mail traffic on a circuit, but block FTP traffic. You can also use ACLs to allow one client to access a part of the network and prevent another client from accessing that same area.

When configuring ACLs, you must apply an ACL to an interface to control traffic on that interface. Applying an ACL on an interface assigns the ACL and its entries to that interface.

You can apply only one extended ACL to each direction (inbound or outbound) of an interface. You can also apply the same ACL on multiple interfaces.You can apply EtherType ACLs in only the inbound direction and on only Layer 2 interfaces.

Note By default, all traffic is denied by the ACE unless explicitly allowed. Only traffic that is explicitly allowed in an ACL can pass. All other traffic is denied.

This section includes the following topics:

- Creating ACLs, page 5-68
- Setting Extended ACL Attributes, page 5-71
- Resequencing Extended ACLs, page 5-75
- Setting EtherType ACL Attributes, page 5-76
- Displaying ACL Information and Statistics, page 5-78

Creating ACLs

You can create an ACL.

Note By default, the ACE denies all traffic unless explicitly allowed. Only traffic that is explicitly allowed in an ACL can pass. All other traffic is denied.

Procedure

Step 1 Choose the item to configure:

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

The ACLs table appears listing the existing ACLs. The ACL fields are described in Table 5-14.

Table 5-14 ACLs Table

Field	Description
Name	Unique identifier for the ACL. Valid entries are unquoted text strings with a maximum of 64 alphanumeric characters.
Type	Identifies the type of ACL as follows: • Extended—Allows you to specify both the source and the destination IP addresses of traffic and the protocol and the action to be taken. For more information see "Setting Extended ACL Attributes" section on page 5-71. • EtherType—This ACL controls network access for non-IP traffic based on its EtherType. An EtherType is a subprotocol identifier. For more information, see the "Setting EtherType ACL Attributes" section on page 5-76.
#	ACL line number for extended type ACL entries.
Action	Action to be taken (permit/deny).
Protocol	Protocol number or service object group to apply to this ACL entry.
Source	Source IP address (and source netmask with port number if configured for extended type ACL) or source network object group (if configured) that is being applied to this ACL entry.
Destination	Destination IP address (and destination netmask with port number if configured for extended type ACL) or destination network object group (if configured) that is applied to this ACL entry.
ICMP	Whether or not this ACL uses ICMP (Internet Control Message Protocol). For more information, see Table 5-17.
Interface	VLAN interfaces associated with this ACL. For example in24,4033:24out where "in" denotes the input direction and "out" denotes the output direction.
Remark	Comments for this ACL.

Step 2 In the ACLs table, do one of the following:

- To view full details of an ACL inline, click the plus sign to the left of any table entry.
- To create an ACL, click **Add**.
- To modify an ACL, choose the radio button to the left of any table entry, and click **Edit**.
- To delete an ACL, choose the radio button to the left of any table entry, and click **Trash**.

If you choose create, the New Access List window appears.

If you choose modify, the Edit ACL or Edit ACL entry window appears based on the selected radio button to the left of any table entry.

Step 3 Add or edit required fields as described in Table 5-15.

Table 5-15 ACL Configuration Attributes

Field	Description
ACL Properties	
Name	Unique identifier for the ACL. Valid entries are unquoted text strings with a maximum of 64 alphanumeric characters.
Type	Type of ACL: • Extended—Allows you to specify both the source and the destination IP addresses of traffic, the protocol, and the action to be taken. For more information see "Setting Extended ACL Attributes" section on page 5-71. • EtherType—This ACL controls network access for non-IP traffic based on its EtherType. An EtherType is a subprotocol identifier. For more information see "Setting EtherType ACL Attributes" section on page 5-76.
Remark	Comments that you want to include for this ACL. Valid entries are unquoted text strings with a maximum of 100 characters. You can enter leading spaces at the beginning of the text or special characters. Trailing spaces are ignored.
ACL Entries	
Entry Attributes	Line number, action and protocol/service object group drop-down list.
Source	Source IP address (and source netmask with port number if configured for extended type ACL) or source network object group (if configured) that is being applied to this ACL entry.
Destination	Destination IP address (and destination netmask with port number if configured for extended type ACL) or destination network object group (if configured) that is applied to this ACL entry.
Add To Table button	Button to add multiple ACL entries, one at a time before clicking **Deploy**.
Remove From Table button	Button to remove multiple ACL entries, one at a time before clicking **Deploy**.
• Input/Output Direction • Currently Assigned (ACL:Direction)	Field that allows you to associate the ACL with one or more interfaces allowing only one input and one output ACL for each interface. The top left checkbox under the Interfaces section allows you to choose and apply to all interfaces "access-group input."
Deploy button	Button to deploy newly created ACL entries and the VLAN interface assignments that were configured.
Cancel button	Button to exit without saving your entries.

Note To add, modify, or delete Object Groups go to the "Configuring Object Groups" section on page 5-79.

Step 4 Do one of the following:

- Click **Deploy** to deploy this newly created ACL entries along with VLAN interface assignments that were configured.
- Click **Cancel** to exit this procedure without saving your entries and to return to the ACLs table.

Related Topics

- Configuring Security with ACLs, page 5-68
- Setting EtherType ACL Attributes, page 5-76
- Setting Extended ACL Attributes, page 5-71
- Resequencing Extended ACLs, page 5-75
- Editing or Deleting ACLs, page 5-87
- Displaying ACL Information and Statistics, page 5-78

Setting Extended ACL Attributes

You can configure extended ACL attributes that allows you to specify both the source and the destination IP addresses of traffic and the protocol and the action to be taken.

For TCP, UDP, and ICMP connections, you do not need to also apply an ACL on the destination interface to allow returning traffic, because the ACE allows all returning traffic for established connections.

Note By default, all traffic is denied by the ACE unless explicitly allowed. Only traffic that is explicitly allowed in an ACL can pass. All other traffic is denied.

Note The ACE does not explicitly support standard ACLs. To configure a standard ACL, specify the destination address as **any** and do not specify the ports in an extended ACL.

Procedure

Step 1 Choose the item to configure:

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

The ACLs table appears, listing the existing ACLs.

Step 2 In the ACLs table, click **Add**.

The New Access List configuration window appears.

Step 3 Click **Add** to add an entry to the table, or choose an existing entry and click **Edit** to modify it.

Step 4 In the ACL Properties pane, enter the ACL name and choose **Extended**.

Step 5 Configure extended ACL entries using the information in Table 5-16.

Table 5-16 Extended ACL Configuration Options

Field	Description
Entry Attributes	
Line Number	Number that specifies the position of this entry in the ACL. The position of an entry affects the lookup order of the entries in an ACL. To change the sequence of existing extended ACLs, see the "Resequencing Extended ACLs" section on page 5-75.

Table 5-16 Extended ACL Configuration Options (continued)

Field	Description
Action	Action to be taken (permit/deny).
Service Object Group	Option that is not applicable to ACE modules running 3.0(0)A1(x) and ACE 4710 appliances running image A1(x). Choose a service object group to apply to this ACL.
Protocol	Protocol or protocol number to apply to this ACL entry. Table 5-17 lists common protocol names and numbers.
Source	
Source Network	Network traffic being received from the source network to the ACE: • Any—Choose the Any radio button to indicate that network traffic from any source is allowed. • IP/Netmask—Use this field to limit access to a specific source IP address. Enter the source IP address that is allowed for this ACL. Enter a specific source IP address and choose its subnet mask. • Network Object Group—Choose a source network object group to apply to this ACL. **Note** This option is not applicable to ACE modules running release 3.0(0)A1(x) and ACE 4710 appliances running release A1(x).
Source Port Operator	Field that appears if you choose TCP or UPD in the Protocol field. Choose the operand to use to compare source port numbers: • **Equal To**—The source port must be the same as the number in the Source Port Number field. • **Greater Than**—The source port must be greater than the number in the Source Port Number field. • **Less Than**—The source port must be less than the number in the Source Port Number field. • **Not Equal To**—The source port must not equal the number in the Source Port Number field. • **Range**—The source port must be within the range of ports specified by the Lower Source Port Number field and the Upper Source Port Number field.
Source Port Number	Field that appears if you choose *Equal To*, *Greater Than*, *Less Than*, or *Not Equal To* in the Source Port Operator field. Enter the port name or number from which you want to permit or deny access. For a list of ports, see the "ANM Ports Reference" section on page A-1.
Lower Source Port Number	Field that appears if you choose *Range* in the Source Port Operator field. Enter the number of the lowest port from which you want to permit or deny access. Valid entries are from 0 to 65535. The number in this field must be less than the number entered in the Upper Source Port Number field.
Upper Source Port Number	Field that appears if you choose *Range* in the Source Port Operator field. Enter the port number of the upper port from which you want to permit or deny access. Valid entries are from 0 to 65535. The number in this field must be greater than the number entered in the Lower Source Port Number field.

Table 5-16 Extended ACL Configuration Options (continued)

Field	Description
Destination	
Destination Network	Network traffic being transmitted to the destination network from the ACE: • Any—Choose the Any radio button to indicate that network traffic to any destination is allowed. • IP/Netmask—Use this field to limit access to a specific destination IP address. Enter the source IP address that is allowed for this ACL. Enter a specific destination IP address and choose its subnet mask. • Network Object Group—Choose a destination network object group to apply to this ACL. **Note** This option is not applicable to ACE modules running release 3.0(0)A1(x) and ACE 4710 appliances running release A1(x).
Destination Port Operator	Field that appears if you choose TCP or UPD in the Protocol field. Choose the operand to use to compare destination port numbers: • **Equal To**—The destination port must be the same as the number in the Destination Port Number field. • **Greater Than**—The destination port must be greater than the number in the Destination Port Number field. • **Less Than**—The destination port must be less than the number in the Destination Port Number field. • **Not Equal To**—The destination port must not equal the number in the Destination Port Number field. • **Range**—The destination port must be within the range of ports specified by the Lower Destination Port Number field and the Upper Destination Port Number field.
Destination Port Number	Field that appears if you choose *Equal To*, *Greater Than*, *Less Than*, or *Not Equal To* in the Destination Port Operator field. Enter the port name or number from which you want to permit or deny access. For a list of ports and keywords, see the "ANM Ports Reference" section on page A-1.
Lower Destination Port Number	Field that appears if you choose *Range* in the Destination Port Operator field. Enter the number of the lowest port to which you want to permit or deny access. Valid entries are from 0 to 65535. The number in this field must be less than the number entered in the Upper Destination Port Number field.
Upper Destination Port Number	Field that appears if you choose *Range* in the Destination Port Operator field. Enter the port number of the upper port to which you want to permit or deny access. Valid entries are from 0 to 65535. The number in this field must be greater than the number entered in the Lower Destination Port Number field.

Table 5-17 Protocol Names and Numbers

Protocol Name[1]	Protocol Number	Description
AH	51	Authentication Header
EIGRP	88	Enhanced IGRP

Table 5-17 Protocol Names and Numbers (continued)

Protocol Name[1]	Protocol Number	Description
ESP	50	Encapsulated Security Payload
GRE	47	Generic Routing Encapsulation
ICMP	1	Internet Control Message Protocol
IGMP	2	Internet Group Management Protocol
IP	0	Internet Protocol
IP-In-IP	4	IP-In-IP Layer 3 Tunneling Protocol
OSPF	89	Open Shortest Path First
PIM	103	Protocol Independent Multicast
TCP	6	Transmission Control Protocol
UDP	17	User Datagram Protocol

[1] For a complete list of all protocols and their numbers, see the Internet Assigned Numbers Authority available at www.iana.org/numbers/.

Step 6 In the Extended configuration pane, do one of the following:

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

Step 7 (Optional) Associate any VLAN interface to this ACL if required and do one of the following:

- Click **Deploy** to immediately deploy this configuration.
- Click **Cancel** to exit without saving your entries and to return to the ACL Summary table.

Related Topics

- Configuring Security with ACLs, page 5-68
- Creating ACLs, page 5-68
- Setting EtherType ACL Attributes, page 5-76
- Resequencing Extended ACLs, page 5-75
- Editing or Deleting ACLs, page 5-87
- Displaying ACL Information and Statistics, page 5-78

Resequencing Extended ACLs

You can change the sequence of entries in an Extended ACL.

Note EtherType ACL entries cannot be resequenced.

Procedure

Step 1 Choose the item to configure:

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

The ACLs table appears, listing the existing ACLs.

Step 2 In the ACLs table, choose the Extended ACL that you want to renumber, and click the **Resequence** icon that appears to the left of the filter field.

The ACL Line Number Resequence window appears.

Step 3 In the Start field of the ACL Line Number Resequence window, enter the number that is to be assigned to the first entry in the ACL.

Valid entries are from 1 to 2147483647.

Step 4 In the Increment field, enter the number that is to be added to each entry in the ACL after the first entry.

Valid entries are from 1 to 2147483647.

Step 5 Do one of the following:

- Click **Resequence** to save your entries and to return to the ACLs table.
- Click **Cancel** to exit this procedure without saving your entries and to return to the ACLs table.

Related Topics

- Configuring Security with ACLs, page 5-68
- Creating ACLs, page 5-68
- Setting EtherType ACL Attributes, page 5-76
- Setting Extended ACL Attributes, page 5-71
- Editing or Deleting ACLs, page 5-87
- Displaying ACL Information and Statistics, page 5-78

Setting EtherType ACL Attributes

You can configure an ACL that controls traffic based on its EtherType, which is a subprotocol identifier. EtherType ACLs support Ethernet V2 frames. EtherType ACLs do not support 802.3-formatted frames because they use a length field instead of a type field. The only exception is a bridge protocol data units (BPDU), which is SNAP encapsulated. The ACE is designed to handle BPDUs.

Note By default, all traffic is denied by the ACE unless explicitly allowed. Only traffic that is explicitly allowed in an ACL can pass. All other traffic is denied.

Procedure

Step 1 Choose the item to configure:

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

The ACLs table appears, listing the existing ACLs.

Step 2 In the ACLs table, click **Add**.

The New Access List configuration window appears.

Step 3 In the ACL Properties pane, enter the ACL name, and choose **Ethertype**.

Step 4 Choose one of the following radio buttons:

- **Deny** to indicate that the ACE is to block connections.
- **Permit** to indicate that the ACE is to allow connections.

Step 5 In the Protocol field, choose one of the following the drop-down list for this ACL:

- **Any**—Specifies any EtherType.
- **BPDU**—Specifies bridge protocol data units. The ACE receives trunk port (Cisco proprietary) BPDUs because ACE ports are trunk ports. Trunk BPDUs have VLAN information inside the payload, so the ACE modifies the payload with the outgoing VLAN if you allow BPDUs. If you configure redundancy, you must allow BPDUs on both interfaces with an EtherType ACL to avoid bridging loops. For information about configuring redundancy, see the "Understanding ACE Redundancy" section on page 12-5.
- **IPv6**—Specifies Internet Protocol version 6.
- **MPLS**—Specifies Multi-Protocol Label Switching. The MPLS selection applies to both MPLS unicast and MPLS multicast traffic. If you allow MPLS, ensure that Label Distribution Protocol (LDP) and Tag Distribution Protocol (TDP) TCP connections are established through the ACE by configuring both MPLS routers connected to the ACE to use the IP address on the ACE interface as the router-id for LDP or TDP sessions. LDP and TDP allow MPLS routers to negotiate the labels (addresses) used to forward packets.

Step 6 Click **Add to Table** and add one or more ACL entries if required repeating Steps 4 and 5 as needed.

Step 7 (Optional) Associate any VLAN interface to this ACL if required and do one of the following:

- Click **Deploy** to immediately deploy this configuration. This option appears for virtual contexts.
- Click **Cancel** to exit without saving your entries and to return to the ACL Summary table.

Related Topics

- Configuring Security with ACLs, page 5-68
- Creating ACLs, page 5-68
- Setting Extended ACL Attributes, page 5-71
- Resequencing Extended ACLs, page 5-75
- Editing or Deleting ACLs, page 5-87
- Displaying ACL Information and Statistics, page 5-78

Displaying ACL Information and Statistics

You can display information and statistics for a particular ACL by using the **Details** button.

Procedure

Step 1 Choose **Config > Devices >** *context* **> Security > ACLs**.

The ACLs table appears listing the existing ACLs.

Step 2 In the ACLs table, choose an ACL, and click **Details**.

The **show access-list** *access-list* **detail** CLI command output appears. For details about the displayed output fields, see either the *Cisco ACE Module Security Configuration Guide* or the *Cisco ACE 4700 Series Appliance Security Configuration Guide*, Chapter 1, Configuring Security Access Control Lists.

Step 3 Click **Update Details** to refresh the output for the **show access-list** *access-list* **detail** CLI command.

Step 4 Click **Close** to return to the ACLs table.

Related Topics

- Configuring Security with ACLs, page 5-68
- Creating ACLs, page 5-68
- Setting Extended ACL Attributes, page 5-71
- Resequencing Extended ACLs, page 5-75
- Editing or Deleting ACLs, page 5-87

Configuring Object Groups

You can configure object groups that you can associate with ACLs. An object group is a logical grouping of objects such as hosts (servers and clients), services, and networks. When you create an object group, you choose a type, such as network or service, and then specify the objects that belong to the groups. In all, there are four types of object groups: Network, protocol, service, and ICMP-type.

After you configure an object group, you can include it in ACLs, thereby including all objects within that group and reducing overall configuration size.

This section includes the following topics:

Creating or Editing an Object Group

You can create a object group or edit an existing one.

Procedure

Step 1 Choose the item to configure:

- To configure a virtual context, choose **Config > Devices >** *context* **> Security > Object Groups**.
- To configure a configuration building block, choose **Config > Global > All Building Blocks >** *building_block* **> Security > Object Groups**.

Note Object groups are available for only ACE modules and ACE module configuration building blocks.

The Object Groups table appears, listing existing object groups.

Step 2 In the Object Groups table, click **Add** to create a new object group, or choose an existing object group, and click **Edit** to modify it.

The Object Groups configuration window appears.

Note The object group definition attributes for Protocol Selection and Service Parameter cannot be edited once defined for an object group. To edit these values, delete the object group definition and then add it again with the desired settings.

Step 3 In the Name field of the Object Groups configuration window, enter a unique name for this object group.

Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.

Step 4 In the Description field, enter a brief description for the object group.

Step 5 In the Type field, choose the type of object group that you are creating:

- **Network**—The object group is based on a group of hosts or subnet IP addresses.
- **Service**—The object group is based on TCP or UDP protocols and ports, or ICMP types, such as echo or echo-reply.

Step 6 Do one of the following:

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

If you click **Deploy Now** or **OK**, the window refreshes with tables additional configuration options.

Step 7 Configure objects for the object group as follows:

- For network-type object groups, options include:
  - Configuring IP Addresses for Object Groups, page 5-80
  - Configuring Subnet Objects for Object Groups, page 5-81
- For service-type object groups, options include:
  - Configuring Protocols for Object Groups, page 5-82
  - Configuring TCP/UDP Service Parameters for Object Groups, page 5-83
  - Configuring ICMP Service Parameters for an Object Group, page 5-85

Configuring IP Addresses for Object Groups

You can specify host IP addresses for network-type object groups.

Note Object groups are available for only ACE modules and ACE module configuration building blocks.

Procedure

Step 1 Choose the item to configure:

- To configure a virtual context, choose **Config > Devices >** *context* **> Security > Object Groups**.
- To configure a configuration building block, choose **Config > Global > All Building Blocks >** *building_block* **> Security > Object Groups**.

The Object Groups table appears, listing the existing object groups.

Step 2 In the Object Groups table, choose the object group that you want to configure host IP addresses for, and click the **Host Setting For Object Group** tab.

The Host Setting for Object Group table appears.

Step 3 In the Host Setting for Object Group table, click **Add** to add an entry to this table.

Step 4 In the Host IP Address field, enter the IP address of a host to include in this group.

Step 5 Do one of the following:

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

Related Topics

- Configuring Object Groups, page 5-79
- Configuring Subnet Objects for Object Groups, page 5-81
- Configuring Protocols for Object Groups, page 5-82
- Configuring TCP/UDP Service Parameters for Object Groups, page 5-83
- Configuring ICMP Service Parameters for an Object Group, page 5-85

Configuring Subnet Objects for Object Groups

You can specify subnet objects for a network-type object group.

Procedure

Step 1 Choose the item to configure:

- To configure a virtual context, choose **Config > Devices >** *context* **> Security > Object Groups**.
- To configure a configuration building block, choose **Config > Global > All Building Blocks >** *building_block* **> Security > Object Groups**.

The Object Groups table appears, listing the existing object groups.

Step 2 In the Object Groups table, choose the object group that you want to configure subnet objects for, and click the **Network Setting For Object Group** tab.

The Network Setting for Object Group table appears.

Step 3 Click **Add** to add an entry to this table.

Step 4 In the IP Address field, enter an IP address that, with the subnet mask, defines the subnet object.

Step 5 In the Netmask field, choose the subnet mask for this subnet object.

Step 6 Do one of the following:

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

Related Topics

- Configuring Object Groups, page 5-79
- Configuring IP Addresses for Object Groups, page 5-80
- Configuring Protocols for Object Groups, page 5-82
- Configuring TCP/UDP Service Parameters for Object Groups, page 5-83
- Configuring ICMP Service Parameters for an Object Group, page 5-85

Configuring Protocols for Object Groups

You can specify protocols for a service-type object group.

Procedure

Step 1 Choose the item to configure:

- To configure a virtual context, choose **Config > Devices >** *context* **> Security > Object Groups**.
- To configure a configuration building block, choose **Config > Global > All Building Blocks >** *building_block* **> Security > Object Groups**.

The Object Groups table appears, listing the existing object groups.

Step 2 In the Object Groups table, choose an existing service-type object group, and click the **Protocol Selection** tab.

The Protocol Selection table appears.

Step 3 In the Protocol Selection table, click **Add** to add an entry to this table.

Step 4 In the Protocol Number field, choose the protocol or protocol number to add to this object group.

See Table 5-17 for common protocols and their numbers.

Step 5 Do one of the following:

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

Related Topics

- Configuring Object Groups, page 5-79
- Configuring IP Addresses for Object Groups, page 5-80
- Configuring Subnet Objects for Object Groups, page 5-81
- Configuring TCP/UDP Service Parameters for Object Groups, page 5-83
- Configuring ICMP Service Parameters for an Object Group, page 5-85

Configuring TCP/UDP Service Parameters for Object Groups

You can add TCP or UDP service objects to a service-type object group.

Procedure

Step 1 Choose the item to configure:

- To configure a virtual context, choose **Config > Devices >** *context* **> Security > Object Groups**.
- To configure a configuration building block, choose **Config > Global > All Building Blocks >** *building_block* **> Security > Object Groups**.

The Object Groups table appears, listing the existing object groups.

Step 2 In the Object Groups table, choose an existing service-type object group, and click the **TCP/UDP Service Parameters** tab.

The TCP/UDP Service Parameters table appears.

Step 3 Click **Add** to add an entry to this table.

Step 4 Configure TCP or UDP service objects using the information in Table 5-18.

Table 5-18 TCP and UDP Service Parameters

Field	Description
Protocol	Protocol for this service object: • TCP—TCP is the protocol for this service object. • TCP And UDP—Both TCP and UDP are the protocols for this service object. • UDP—UDP is the protocol for this service object.
Source Port Operator	Operand to use when comparing source port numbers for this service object: • Equal To—The source port must be the same as the number in the Source Port field. • Greater Than—The source port must be greater than the number in the Source Port field. • Less Than—The source port must be less than the number in the Source Port field. • Not Equal To—The source port must not equal the number in the Source Port field. • Range—The source port must be within the range of ports specified by the Lower Source Port field and the Upper Source Port field.
Source Port	Field that appears if you choose Equal To, Greater Than, Less Tha*n*, or Not Equal To in the Source Port Operator field. Enter the source port name or number for this service object.
Lower Source Port	Field that appears if you choose Range in the Source Port Operator field. Enter the number that is the beginning value for a range of services for this service object. Valid entries are from 0 to 65535. The number in this field must be less than the number entered in the Upper Source Port field.
Upper Source Port	Field that appears if you choose Range in the Source Port Operator field. Enter the number that is the ending value for a range of services for this service object. Valid entries are from 0 to 65535. The number in this field must be greater than the number entered in the Lower Source Port field.

Table 5-18 TCP and UDP Service Parameters (continued)

Field	Description
Destination Port Operator	Operand to use when comparing destination port numbers: • **Equal To**—The destination port must be the same as the number in the Destination Port field. • **Greater Than**—The destination port must be greater than the number in the Destination Port field. • **Less Than**—The destination port must be less than the number in the Destination Port field. • **Not Equal To**—The destination port must not equal the number in the Destination Port field. • **Range**—The destination port must be within the range of ports specified by the Lower Destination Port field and the Upper Destination Port field.
Destination Port	Field that appears if you choose Equal To, Greater Than, Less Than, or Not Equal To in the Destination Port Operator field. Enter the destination port name or number for this service object.
Lower Destination Port	Field that appears if you choose Range in the Destination Port Operator field. Enter the number that is the beginning value for a range of services for this service object. Valid entries are from 0 to 65535. The number in this field must be less than the number entered in the Upper Destination Port field.
Upper Destination Port	Field that appears if you choose Range in the Destination Port Operator field. Enter the number that is the ending value for a range of services for this service object. Valid entries are from 0 to 65535. The number in this field must be greater than the number entered in the Lower Destination Port field.

Step 5 Do one of the following:

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

Related Topics

- Configuring Object Groups, page 5-79
- Configuring IP Addresses for Object Groups, page 5-80
- Configuring Subnet Objects for Object Groups, page 5-81
- Configuring Protocols for Object Groups, page 5-82
- Configuring ICMP Service Parameters for an Object Group, page 5-85

Configuring ICMP Service Parameters for an Object Group

You can add ICMP service parameters to a service-type object group.

Procedure

Step 1 Choose the item to configure:

- To configure a virtual context, choose **Config** > **Devices** > *context* > **Security** > **Object Groups**.
- To configure a configuration building block, choose **Config** > **Global** > **All Building Blocks** > *building_block* > **Security** > **Object Groups**.

The Object Groups table appears, listing the existing object groups.

Step 2 In the Object Groups table, choose an existing service-type object group, and click the **ICMP Service Parameters** tab.

The ICMP Service Parameters table appears.

Step 3 Click **Add** to add an entry to this table.

Step 4 Configure ICMP type objects using the information in Table 5-19.

Table 5-19 ICMP Type Service Parameters

Field	Description
ICMP Type	ICMP type or number for this service object. Table 5-20 lists common ICMP types and numbers.
Message Code Operator	Operand to use when comparing message codes for this service object: • **Equal To**—The message code must be the same as the number in the Message Code field. • **Greater Than**—The message code must be greater than the number in the Message Code field. • **Less Than**—The message code must be less than the number in the Message Code field. • **Not Equal To—**The message code must not equal the number in the Message Code field. • **Range**—The message code must be within the range of codes specified by the Min Message Code field and the Max. Message Code field.
Message Code	Field that appears if you choose Equal To, Greater Than, Less Than, or Not Equal To in the Message Code Operator field. Enter the ICMP message code for this service object.
Min. Message Code	Field that appears if you choose Range in the Message Code Operator field. Enter the number that is the beginning value for a range of services for this service object. Valid entries are from 0 to 255. The number in this field must be less than the number entered in the Max Message Code field.
Max. Message Code	Field that appears if you choose Range in the Message Code Operator field. Enter the number that is the ending value for a range of services for this service object. Valid entries are from 0 to 255. The number in this field must be greater than the number entered in the Min. Message Code field.

Table 5-20 ICMP Type Numbers and Names

Number	ICMP Type Name
0	Echo-Reply
3	Unreachable
4	Source-Quench
5	Redirect
6	Alternate-Address
8	Echo
9	Router-Advertisement
10	Router-Solicitation
11	Time-Exceeded
12	Parameter-Problem
13	Timestamp-Request
14	Timestamp-Reply
15	Information-Request
16	Information-Reply
17	Address-Mask-Request
18	Address-Mask-Reply
31	Conversion-Error
32	Mobile-Redirect

Step 5 Do one of the following:

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

Related Topics

- Configuring Object Groups, page 5-79
- Configuring IP Addresses for Object Groups, page 5-80
- Configuring Subnet Objects for Object Groups, page 5-81
- Configuring Protocols for Object Groups, page 5-82
- Configuring TCP/UDP Service Parameters for Object Groups, page 5-83

Managing ACLs

This section describes how to manage ACLs.

This section includes the following topics:

- Viewing All ACLs by Context, page 5-87.
- Editing or Deleting ACLs, page 5-87.

Viewing All ACLs by Context

You can display ACLs that have been configured.

Procedure

Step 1 Choose **Config > Devices**.

The device tree appears.

Step 2 In the device tree, choose the virtual context with the ACLs that you want to view, and choose **Security > ACLs**.

The ACLs table appears, listing the existing ACLs in that context with their name, their type (Extended or EtherType), and all details (such as Action, Protocol, Interface information).

Step 3 To display all of the ACLs for a given table entry, click the plus sign to the left of that entry.

Step 4 To display all of the ACLs for all of the entries, click **Expand All** on the Add/Edit/Delete row.

Step 5 To collapse all of the ACLs for all of the entries, click **Collapse All** on the Add/Edit/Delete row.

Related Topics

- Configuring Security with ACLs, page 5-68
- Creating ACLs, page 5-68
- Setting EtherType ACL Attributes, page 5-76
- Setting Extended ACL Attributes, page 5-71
- Editing or Deleting ACLs, page 5-87

Editing or Deleting ACLs

You can delete or edit an ACL or any of its subentries.

Procedure

Step 1 Choose the item to edit or delete as follows:

- Choose **Config > Devices >** *context* **> Security > ACLs**.
- Choose **Config > Global > All Building Blocks >** *building_block* **> Security > ACLs**.

The ACLs table appears, listing the existing ACLs.

Step 2 In the ACLs table, choose the radio button to the left of the ACL that you want to Edit or Delete.

Expand entries if necessary by clicking the plus sign to the left of any ACL entry until you see the subentry ACL for which you are looking, or click the **Expand All** icon to view all ACLs and subentries.

Step 3 Do one of the following:

- If you are editing an ACL or one of its entries, click **Edit** and go to Step 4.
- If you are deleting an ACL or one of its entries, click **Delete** and go to Step 5.

Step 4 Edit the entry using the summary information listed in Table 5-15 if needed, and click **Deploy** when done.

Step 5 Click **Delete**.

A confirmation popup window appears asking you to confirm the deletion. If you click **OK**, the ACLs table refreshes without the deleted ACL.

Related Topics

- Creating ACLs, page 5-68
- Setting EtherType ACL Attributes, page 5-76
- Setting Extended ACL Attributes, page 5-71
- Resequencing Extended ACLs, page 5-75

Configuring Virtual Context Expert Options

The ANM virtual context Expert configuration options allow you to do the following:

- Establish traffic policies for virtual servers by classifying types of network traffic and then applying the appropriate rules and actions for handling the traffic. See the "Configuring Traffic Policies" section on page 13-1.
- Compare a virtual context configuration with a tagged configuration building block that has been applied to the context. See the "Comparing Context and Building Block Configurations" section on page 5-88.
- For ACE modules and ACE appliances, configure HTTP header modify action lists. See the "Configuring an HTTP Header Modify Action List" section on page 13-83.
- For ACE appliances, configure optimization action lists. See the "Configuring an HTTP Optimization Action List" section on page 14-3.

Comparing Context and Building Block Configurations

ANM allows you to compare the current configuration of a virtual context that has had a tagged configuration building block applied to it with the settings of the applied building block. Discrepancies between these configurations can occur when you configure the virtual context after applying the building block instead of modifying and tagging the building block, then applying the updated building block to the virtual context.

The ANM auditing process identifies the discrepancies by configuration category (such as policy maps or SNMP) and groups them accordingly.

You can identify discrepancies between an ANM tagged building block and a virtual context that previously had the building block applied to it.

Assumption

The virtual context has had a tagged building block applied to it.

Procedure

Step 1 Choose **Config > Devices >** *context* **> Expert > Building Block Audit**.

The Building Block Audit window appears with the Comparison Results table, listing any discrepancies between the configurations.

Step 2 In the Building Block Audit window, identify the discrepancies as follows:

- Click **All** at the top of the results tree. The Comparison Results table displays all discrepancies.

  The values that follow the word All, such as 2c 5d 3a, indicate differences between the virtual context configuration and the building block configuration. These values use the format *n<difference>* where *n* represents the number of differences between the configurations and *<difference>* represents the type of difference. The possible results are as follows:

  – *n*c (changed) indicates the number of items with settings that have changed or differ from the settings in the building block. For example, 2c indicates that two configuration options in the context currently have different settings or values than those settings or values in the applied building block.

  – *n*d (deleted) indicates the number of items that were in the applied building block that do not exist in the current context configuration. For example, 5d indicates that five configuration options that were in the applied building block do not exist in the current context configuration.

  – *n*a (added) indicates the number of items that are in the current context configuration that were not in the applied building block. For example, 3a indicates that three configuration options that were not in the applied building block have been added to the context configuration.

- Click a folder in the results tree. The Comparison Results table displays the discrepancies for that configuration category, such as SNMP or class maps.
- Click an item within a folder. The Comparison Results table displays the differences for that specific attribute.

Step 3 In the Comparison Results table, when viewing results, you can do one of the following:

- Filter the results by entering a complete or partial string in one or more of the input fields at the top of the columns, then clicking **Go**.
- Sort the results in ascending or descending order by clicking a column heading.

Related Topics

- Configuring Virtual Contexts, page 5-7
- Managing Virtual Contexts, page 5-90
- Using Configuration Building Blocks, page 15-1

Managing Virtual Contexts

You can perform the following administrative actions on virtual contexts.

This section includes the following topics:

- Displaying All Virtual Contexts, page 5-90
- Synchronizing Virtual Context Configurations, page 5-92
- Managing Syslog Settings for Autosynchronization, page 5-92
- Editing Virtual Contexts, page 5-93
- Deleting Virtual Contexts, page 5-94
- Upgrading Virtual Contexts, page 5-94
- Restarting Virtual Context Polling, page 5-95
- Comparing Context and Building Block Configurations, page 5-88

Displaying All Virtual Contexts

You can display some or all virtual contexts being managed by ANM.

Procedure

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

The All Virtual Contexts table appears with the information described in Table 5-21.

Table 5-21 All Virtual Contexts Table

Field	Description
Name	Context name including chassis and slot.
Resource Class	Resource class applied to the context.
Management IPs	List of IP addresses used for remote management of the context.
Building Block	Configuration building block applied to the context.
CLI Sync Status	Administrative configuration status of the context as follows: • Import Failed—The context did not import successfully. This problem could have occurred when the device was added to ANM or when the context was synchronized. Synchronize the context so that you can manage it (**Config > Devices >** *ACE* **>** *context* **> Sync**). • OK—The context is synchronized with the ACE CLI. • Out of Sync—The context is managed by the ANM but the configuration for the context on the device differs from the configuration managed by the ANM. For information on synchronizing contexts, see the "Synchronizing Virtual Context Configurations" section on page 5-92. • Unprovisioned—The context has been removed from the ACE using the CLI but has not been removed from ANM. To remove unprovisioned contexts, synchronize the associated Admin context.
Last CLI Sync Status Change	Time stamp of the last CLI synchronization with ANM.

Table 5-21 All Virtual Contexts Table (continued)

Field	Description
ACE HA State	High availability state of the context. If the context is configured for high availability, the current state of the context with regard to high availability: • Active—The context is actively processing flows for the HA pair. • Standby Cold—Either the fault-tolerant VLAN is down, but the peer ACE is still alive, or the configuration or application state synchronization failed. • Standby Bulk—The context is waiting to receive information from its active peer context. • Standby Hot—The context has all the state information that it needs to statefully assume the active state if a switchover occurs. • Standby Warm—Allows the configuration and state synchronization process to continue on a best-effort basis when you upgrade or downgrade the ACE software.
ACE HA Peer	Identifier of the ACE high availability peer.
ACE HA Peer State	Current state of the context with regard to high availability on the ACE peer. See the states listed for the ACE HA State field.
Polling Status	Current polling status of the context: • Missing SNMP Credentials—SNMP credentials are not configured for this virtual context; statistics are not collected. Add SNMPv2c credentials to fix this error. • Not Polled—SNMP polling has not started. This problem might occur when the virtual context is first created from ANM and the SNMP credentials are not configured. Add SNMPv2c credentials to fix this error. • 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 restarting polling to enable SNMP collection again. • Polling Started—No action is required. Everything is working properly. Polling states will display activity. • Polling Timed Out—SNMP polling has timed out. This problem might occur if the wrong credentials were configured or might be caused by an internal error (such as SNMP was configured incorrectly or the destination is not reachable). Verify that SNMP credentials are correct. If the problem persists, restart polling to enable SNMP collection again. • Unknown—SNMP polling is not working due to one of the above-mentioned conditions. Check the SNMPv2c credential configuration.

Step 2 Use the object selector to view all virtual contexts or only those contexts on a specific device.

Related Topics

- Restarting Virtual Context Polling, page 5-95
- Enabling Polling on All Devices, page 16-43
- Synchronizing Virtual Context Configurations, page 5-92

Synchronizing Virtual Context Configurations

You can synchronize the configurations for a virtual context. ANM allows you to synchronize the configuration information residing on an ACE with the configuration information maintained by the ANM server for the same device. When ANM synchronizes a context, it uploads the configuration from the device to the ANM server. In accordance with your role-based permission level, the ANM Status bar displays the number of virtual contexts that are not synchronized with the ACE CLI against the total number of virtual contexts and the number of failed synchronization attempts.

You should synchronize contexts for the following reasons:

- You configure the ACE directly via the CLI instead of using the ANM interface. The CLI Sync Status is *Out of Sync* in the Virtual Contexts table (**Config > Devices >** ACE) if the configurations for a virtual context differ.
- A context has been removed from the ACE using the CLI, reflected by the CLI Sync Status *Unprovisioned* in the Virtual Contexts table. In this situation, you need to synchronize the Admin context to remove the unprovisioned context.
- A context has not successfully been imported into ANM during discovery or a Sync operation, reflected by the CLI Sync Status *Import Failed* in the Virtual Contexts table. In this situation, you need to synchronize the context before you can modify its configuration.
- You recently installed or uninstalled a license on an ACE using either ANM or the CLI. Synchronize the Admin context of the ACE with the CLI.

Procedure

Step 1 Choose **Config > Devices**.

The device tree appears.

Step 2 In the device tree, choose either **All VC** or the ACE with the virtual context configuration that you want to synchronize.

The Virtual Contexts table appears.

Step 3 In the Virtual Contexts table, choose the virtual context with the configuration that you want to synchronize, and click **CLI Sync**.

The Virtual Contexts table refreshes when synchronization is complete.

Related Topics

- Configuring Auto Sync Settings, page 17-85
- Editing Virtual Contexts, page 5-93
- Restarting Virtual Context Polling, page 5-95
- Comparing Context and Building Block Configurations, page 5-88

Managing Syslog Settings for Autosynchronization

You can configure ANM to receive syslog messages for a virtual context.

Setting autosynchronization to occur upon receipt of a device syslog message allows a faster, more streamlined synchronization process between ANM and any out-of-band configuration changes. Instead of waiting the default polling period, ANM will synchronize when a syslog message is received if Setup Syslog for Autosync is enabled.

Procedure

Step 1 Choose **Config > Devices > Virtual Context Management> Setup Syslog for Autosync**.

The Setup Syslog for Autosync window appears.

Step 2 In the Setup Syslog for Autosync window, choose either **All VC** or the ACE with the virtual context configuration that you want to receive Autosync syslog messages

Step 3 Click **Setup Syslog**.

A progress bar window appears.

A checkbox with a checkmark appears in the Setup Syslog for Autosync? column for each virtual context and ACE device you checked.

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

The following CLI commands are sent to the enabled devices:

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

Related Topics

- Synchronizing Virtual Context Configurations, page 5-92
- Restarting Virtual Context Polling, page 5-95

Editing Virtual Contexts

You can modify the configuration of an existing virtual context.

Procedure

Step 1 Choose **Config > Devices.**

The device tree appears.

Step 2 In the device tree, choose the virtual context, then choose the configuration attributes that you want to modify.

For information on configuration options, see the "Configuring Virtual Contexts" section on page 5-7.

Step 3 Do one of the following:

- Click **OK** to save your entries.
- Click **Cancel** to exit the procedure without saving your entries.

Related Topics

- Information About Virtual Contexts, page 5-2
- Configuring Virtual Contexts, page 5-7

Deleting Virtual Contexts

You can remove an existing virtual context.

Note If you remove a virtual context using the CLI, the CLI Sync Status for the virtual context appears as Unprovisioned in the Virtual Contexts table (Config > Devices > ACE). To remove the unprovisioned virtual context from the ANM, either synchronize the Admin virtual context (see the "Synchronizing Virtual Context Configurations" section on page 5-92) or delete the virtual context by selecting the virtual context, then clicking **Delete**.

Procedure

Step 1 Choose **Config > Devices**.

The device tree appears.

Step 2 In the device tree, choose the virtual context that you want to configure, and click **Delete** in either the device pane or the configuration pane.

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

Step 3 Do one of the following:

- Click **OK** to delete the selected context. The device tree refreshes and the deleted context no longer appears.
- Click **Cancel** to exit this procedure and to retain the selected context.

Related Topics

- Configuring Virtual Contexts, page 5-7
- Comparing Context and Building Block Configurations, page 5-88

Upgrading Virtual Contexts

You can apply a different resource class, configuration building block, or VLAN to a virtual context.

Procedure

Step 1 Choose **Config > Devices**.

The device tree appears.

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

The Edit Virtual Context window appears.

Step 3 In the Resource Class field of the Edit Virtual Context window, choose the resource class that you want to apply to the context.

> **Note** If you attempt to apply a resource class that could consume the resources required to maintain IP connectivity to the Admin context, you will see an error message and the resource class will not be applied. We recommend that you first apply a resource class to the Admin context that will prevent its resources from being allocated to other contexts. For more information, see the "Resource Allocation Constraints" section on page 5-42.

Step 4 In the Tagged Building Block To Apply field, choose the building block to apply to this virtual context.

Step 5 In the Allocate-Interface VLANs field, enter the number of a VLAN or a range of VLANs so that the context can receive the associated traffic.

You can specify VLANs as follows:

- For a single VLAN, enter an integer from 2 to 4096.
- For multiple, nonsequential VLANs, use comma-separated entries, such as 101,201,302.
- For a range of VLANs, use the format <*beginning-VLAN*>-<*ending-VLAN*>*,* such as 101-150.

> **Note** You cannot modify VLANs in an Admin context.

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

Step 7 Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.

The window refreshes with updated information.

To exit this procedure without saving your entries, choose another item in the menu bar or device tree. A popup window appears, confirming that you have not saved your entries.

Related Topics

- Information About Virtual Contexts, page 5-2
- Configuring Virtual Contexts, page 5-7

Restarting Virtual Context Polling

You can restart monitoring and enable SNMP collection on a single context that has stopped or failed to start.

> **Note** To restart polling and enable SNMP collection on all virtual contexts, choose **Monitor > Settings > Global Polling Configuration**, and configure global polling attributes using the information in the "Enabling Polling on All Devices" section on page 16-43.

Procedure

Step 1 Choose **Config > Devices**.

The device tree appears.

Step 2 In the device tree, choose the ACE associated with the virtual context with stopped or failed polling.

The Virtual Contexts table appears.

Step 3 In the Virtual Contexts table, choose the context with the stopped or failed polling, and click **Restart Polling**.

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

Related Topics

- Information About Virtual Contexts, page 5-2
- Configuring Virtual Contexts, page 5-7
- Enabling Polling on All Devices, page 16-43